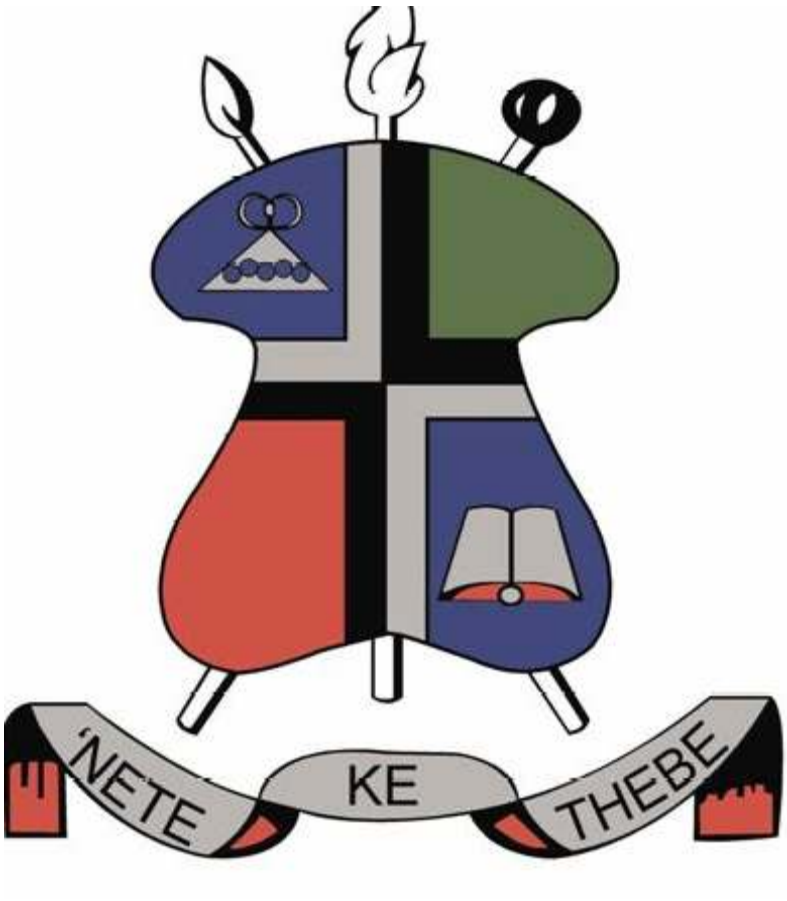

Networks Management Course Manual

Lekulana Kolobe

Department of Mathematics and Computer Science
The National University of Lesotho, Maseru, Roma

CS5440 – 2007

1.0. Introduction to Networks Management

1.0.1. Definitions of Engineering

Several definitions are available on the web and other resources of the discipline "*engineering*", including the following:

a) The practical application of science to commerce or industry;
b) A discipline dealing with the art or science of applying scientific knowledge to practical problems;
c) Application of science to the needs of humanity, accomplished through the application of knowledge, mathematics, and practical experience to the design of useful objects or processes;
d) Field concerned with putting scientific knowledge to practical needs;
e) Etc.

The most important component of engineering is "*how society is affected by the scientific knowledge, not the scientific knowledge itself*". So, when studying engineering, students are expected, in all of their problem solving and projects, to consider how the particular technology affects the general public (society), environment, health issues, politics, policies, economics, etc. So, for a project or research to meet the engineering standard, the author or engineer must have considered:

a) How is the society affected by the technology?
b) Is it economically viable?
c) How does it affect our fragile environment?
d) Does it contribute towards employment creation?
e) What are the health issues associated with it?
f) Global warming, community eyesore, etc.

1.0.2. What is Networks Management?

Networks management defines all activities involved in providing, monitoring, interpreting, maintaining, controlling and supervising the network and the services it carries. These activities include functions form operations, administration, maintenance and provisioning (OAM&P) [24]. All in all, these functions provide operators, corporate customers (businesses) and end-users with efficient and effective means to manage their resources and services to achieve objectives and meet the levels agreed in SLAs.

Other definitions from the web include:

a) "*The process of controlling a network so as to maximize its efficiency and productivity*";
b) "*The execution of the set of functions required for controlling, planning, allocating, deploying, coordinating and monitoring networks*".

1.0.3. Roles of a Network Manger

Network managers perform all duties relating to the management of network infrastructure, partners, and the personnel involved in the network and include:

a) Plan, design, implement, test, maintain and control the network;
b) Creates and enforces management and security policies;
c) Maximizes the use of scarce resources and minimizes costs associated with the whole network;
d) Monitors network performance and oversees the network;
e) Plan and document backup, disaster and data recovery policies and strategies;
f) Manage the ICT staff;
g) Allocates of duties to the network administrator and other ICT staff;
h) Makes location-based decisions regarding placement of help/service desks and call centers;
i) Draws up contracts with vendors and suppliers (partners);
j) Performs all activities in supply-chain management regarding ICT infrastructure;
k) Ensures legal and regulatory adherence of the network and its services;
l) Ensures that ICT equipment and services meet international standards;
m) Monitors all the five management areas of FCAPS;
n) Sits in meetings with higher management and reports to them regarding ICT matters.

Exercise: *Differentiate between network manager and network administrator*.

1.0.4. Why Manage Networks?

Several reasons or factors have necessitated the need to continuously manage the networks used for offering services to customers. Only experimental or laboratory based networks do not require management, but all other network settings do. Key among the reasons is the dependence of most organizations, businesses and individuals on the proper operation of networks, and the need to offer quality services by network operators. Quality in this case is used as the ability of a service to continuously meet the expectations of the customer. These factors include the following:

a) Network dependence of universities, schools, businesses, health sector, banking, military, emergency services, stock exchange, etc;
b) Control and optimize the operation of the network;
c) To respond to changing user requirements;
d) Timeously attend to faults and disruptions, so as not to hinder productivity;
e) Ensure efficient and effective use and sharing of resources;
f) Fair access to scarce networked resources;
g) The ever-growing networks and the need to manage complexity;
h) Heterogeneous protocols, devices, vendors, etc;
i) Maintain control of ICT infrastructure (corporate asserts);
j) To avoid loss of network resources and poor performance.

Several examples of network problems have been experienced by several companies in recent years, including Vodacom SA network collapse of 2006; Johannesburg Stock Exchange (JSE) in July 2008 [26], and July 2010 [29]; Heathrow Airport [27, 28] delay in February 2008; etc.

Trading on JSE resumes [26]

Will continue until 19h00. Loubser says "*we really are very sorry*".

David Carte
14 July 2008 00:00

Trading on the JSE (JSE:JSE) resumed at 15h10 today after a network related problem stopped trade from 06h30. Trading will continue until 19h00 today. JSE president Russell Loubser said he knew that the interruption was hugely inconvenient to thousands of parties and apologized profusely. "We have been working on the problem flat out since 06h30. We hardly had time to apologize but we really are very sorry. We think we have resolved it now."
Loubser said he was disappointed at the computer crash because it dented the JSE network's *100%* record of constant availability for the past six years. The trading system's *99% record* would also be impaired. Loubser said JSE officials always knew the problem was in the network, as opposed to the trading system. The network comprises both hardware and software and it was not immediately clear what the problem was. He said it would be difficult to describe the problem in three seconds. "I suppose we have to realise that even the best systems can go wrong. NASA lost a space shuttle or two and they are the best." Loubser said many stock exchanges suffered interruptions of this kind. They hate it and try to avoid it.
"We'll be making humble apologies to everyone affected in the near future."

Delays reported at Heathrow Airport due to computer crash **[27]**
Airline Industry Information, Feb 21, 2008

A baggage system computer which crashed led to the delay of a number of passengers yesterday (20 February) at London's Heathrow Airport.
An upgrade of the automatic baggage sorting system's computer in Terminal 4, reportedly led to the system crashing on Tuesday (19 February), with workers being unable to place traveller's luggage in the correct area to be sorted.
The problem led to delays for a larger number of passengers, particularly those travelling on long-haul flights with British Airways.
According to The Associated Press, airport operator BAA said that the computer problem would be fixed by Thursday (21 February).

Photo apparently taken by Alan Cox at Heathrow International Airport, London, England; arrived over the Net. ***Aren't you glad that planes don't fly by Windows***? [28]

JSE Shakes Off Technical Glitch
Business News form News24; July 13, 2010.

ON Monday July 12, 2010, Johannesburg Stock Exchange delayed the start of equity trading by 90 minutes due to a problem with its international connectivity, which is managed by MTN SA. It is not the first time that JSE is hit by technical woes. In September 2008, it halted trading for several hours due to connectivity problems. In March its regulatory news service failed to update for several hours. [29]

1.0.5. Drivers for Networks Management

The key driver in modern networks is change, which occurs in services, applications, networks, etc. Due to these changes the following are diving networks management [24]:

a) Services Evolution – new services are emerging daily including pay-per view video, video-on-demand, video conferencing, virtual private networks, etc.
b) Technology Evolution – support for multifunctional, single networks, and evolving transport systems such as NG-SDH, Advanced IN, etc.
c) Customer Requirements – bandwidth-on-demand, service-on-demand, etc; fast service provisioning and easy DIY installations regardless of their location.
d) Competitiveness – the need to reduce network costs, yet improve services delivery and improved quality; streamline implementation of new services and identifying new revenue-generating opportunities.

1.1. Concepts and History of Telecommunications

1.1.1. Concepts as used

Several concepts in the field of networking are misinterpreted and some have more than one meaning depending on the user. To avoid any confusion, the following concepts are defined:

a) Communication – any means used for the transfer or exchange of comprehensive information. Examples include [4]: reading of books, newspapers and notice boards; transport facilities such as buses, trains, taxis and planes; telephone calls; radios; TVs; post offices; etc.
b) Network – "*the total infrastructure, both hardware and software required to deliver specified services*" [19]. Two types of networks are voice and data networks; however, modern and future networks aim to provide a single network capable of supporting voice, data, video and multimedia.
c) Telecommunications – derived from the word "*tele*", which means "*remote*", i.e. bridging the geographical distance. So, telecommunications means "*the remote exchange of comprehensive information*" [4].
d) Telecommunications Technology – "*an established body of knowledge, concepts and principles, implemented in hardware and software as required, in order to meet a connection, control, service or management need*" [19]. Technologies can either be [19]:

    i. Legacy – technologies which, while obsolescent are still in use in the network;
    ii. Current – technologies are not yet obsolete and must co-exist and interwork with legacy types;
    iii. Emerging – technologies that are not yet fully proven or implemented.

e) Network Operator – a company that administers a telecommunications network.

Telecommunications industry is referred to as an "*enabling industry*", because it creates opportunities for societal development and several projects worldwide are underway, which show the importance of this field in poverty reduction, HIV/AIDS awareness, etc.

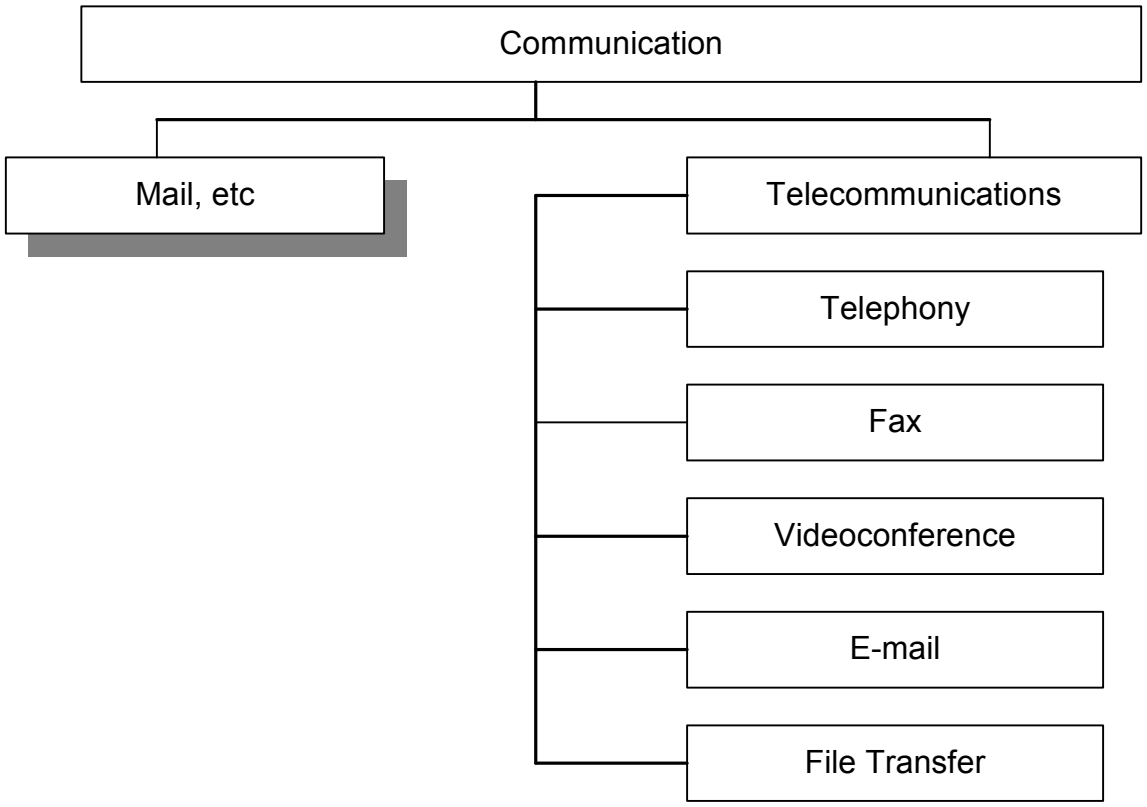

Figure 1.0.1, [4], clarifies communications and telecommunications

1.1.2. Historical Milestones in Telecommunications

1980	First fully electronic telephone exchange deployed
	First optic fibre cable deployed
1981	First Mobile Telephone
1982	TCP selected for ARPANET
1984	Break up of AT&T into Regional & long distance operators
	1000 hosts on the Internet
1988	Principle of Asynchronous Transfer mode established
	Standardization of ISDN
1990	Specification of Frame Relay
1991	World Wide Web launched
1992	GSM Mobile networks deployed
	1 million hosts on the Internet
1995	10 million hosts on the internet
	Web traffic overtakes any other
1999	IPv6 deployed world wide
2000	First licences for 3rd Generation Mobile networks
2002	140 million hosts on the Internet
2004	
2006	
2015-2020	Global Connection? Everybody connected? No digital divide?

Table 1.1.1, adapted from [19] shows historical milestones in telecommunications since 1980

1.2. Telecommunication Networks Management

1.2.1. Introduction

Just like all other ICT infrastructure, public telecommunications networks need to be managed, supervised and controlled. The control and supervision were traditionally referred to as "*operations and maintenance*" [4]. In recognition to this, most companies today still have divisions dedicated to operations and maintenance or simply operations management divisions. No matter how they are called, operations and maintenance satisfy two (2) key objectives namely [4]:

a) To enable the telecommunications network to provide customers with services they demand satisfactorily, thus creating a happy customer experience;
b) To enable the operator to monitor the provided services and to offer them in the most cost-effective manner.

In order for the operator to provide the customer with the required or agreed upon services, the operations part is involved and consists of the following:

a) Subscriber Management – before services can be offered, the operator has to first connect subscribers, modify subscriber details, move subscribers, and finally terminate subscribers.
b) Charging – before the subscriber can be charged for the services, the operator must be able to effectively and accurately collect the charging information, so that each customer is correctly billed only for the services used. Billing information is very important as it forms "*the basis of the operator's revenue-earning or revenue-generating scheme, and is collected several times during a 24-hour period*" [14].
c) Traffic Management – for subscribers to adequately receive quality services, agreed upon in SLAs, Teletraffic must be distributed in a way that improves grade of service and the degree of network utilization, while minimizing the risk of overload [4].
d) Signalling Functions – all activities that involve call setup, call monitoring and termination, traffic switching, activations and disconnection of services.
e) Service Management – after offering services, operators have to ensure that they are available and reliable and of the required standard, so as to maintain high subscriber satisfaction.

In addition to operations activities, operators also have to perform maintenance activities to keep services as required by the subscribers. The key objective of maintenance is "*to provide against faults and disturbances in the network and to correct actual faults when they occur*" [4]. There are two (2) types of maintenance activities namely [4]:

a) Corrective – reacts to actual faults by first locating the fault (through troubleshooting) and then correcting the fault;
b) Preventive – monitors the network to see when the services offered start to deteriorate and it involves regular measurements of traffic statistics and supervision of the entire telecommunications network. Among the monitored metrics, include bit error rates, probability of congestion, likelihood of failure, etc.

Previously, operations and maintenance activities have been decentralized i.e. distributed as opposed to being in the single centralized location, however, this decentralization contributed to too much expense as evidenced by the following quote: "*O&M work entails great expense – often 60-70% of the operator's total costs – which is attributable to three partly interacting factors: staff costs, decentralization, and over dimensioning of the telecommunications networks*" [4]. To avoid these costs and other downfalls of decentralization, the O&M activities are now centralized into a single location and this is achieved by the system called operations support system (OSS) [4]. OSSs are capable of remotely controlling and supervising several network elements (exchanges in the public network) and clearly this offers several benefits when opposed to the previous decentralized systems. This centralization offers several benefits including:

a) Reduced staff, thus leading to reduced expenses;
b) Easily handle functions in a single location;
c) Automation of services can be easily achieved;
d) Upgrade of the O&M is easy and controllable.

Realizing the benefits offered by OSS, most companies have already implemented OSS and several others are following suit, like Telecom Lesotho, which has already placed two (2) advertisements in Public Eye newspaper, Vol. 11, No.27, dated 6th July 2006, requesting companies with expertise in OSS to provide information regarding OSS in the form of RFC and RFI.

Request For Information – TL/RFI/NDP/April-07001/01

RFI for the establishment of Operational Support System (OSS) in Lesotho

1. Request for Information (RFI):

Telecom Lesotho (TL), a Fixed Network operator in Lesotho and its subsidiary, Econet Ezicel Lesotho (EEL), a GSM network operator, wish to implement an Operational Support System – OSS as a means of providing single operating center to monitor, control, analyze and manage a telephone and computer network. As the traditional voice telephone systems converge with packet-oriented Internet traffic (Including VoIP), broadband applications such as teleconferencing, DSL and ADSL, operators need more sophisticated systems like OSS to consolidate multitude of proprietary network management systems (NMS) for rapid response for ordering and tracking network components (IP addresses), usage and tracking network traffic patterns, billing and reporting. This RFI invites input and ideas from renowned manufacturers and suppliers of OSS to assist TL and EEL achieve their objective.

2. Network:

Telecom Lesotho operates traditional fixed network comprising legacy equipment in the switch and a mixture of legacy and next generation (NG) in the transmission. The switches are all Ericsson made while transmission is made up of various microwave- and fibre-based PDH & SDH/NG-SDH systems. Data network is built on three systems supplied by different vendors. There are currently twelve (12) NMS terminals used to manage the network. EEL operates a GSM network comprising a Softswitch, base station controller and base stations all from one vendor, and value services platforms comprising a Prepaid System, SMSC and VMS all from another vendor. It is required that the RFI should aim at OSS that will provide solutions for the present and future needs. It is worth to mention that TL has vigorously engaged in network transformation toward building NGN and EEL will also be introducing mobile data services through GPRS, EDGE and 3G technology.

***3. Eligibility**:*

The invitation applies to all Local and International companies [or any of their accredited agents or representatives with proven track experience] who have the necessary experience in the manufacture of OSS and or TMN equipment.

4. Submission of Response to RFI

a) *The responses to RFI must reach Telecom Lesotho on or before Thursday 12th July at 12:00 hrs at the latest*
b) *Response Documents should be e-mail to Tendercommittee@telecom.co.ls*
c) *Submission of Response Documents does not in anyway bind Telecom Lesotho into any conditions.*

5. Correspondence and Queries

All correspondences and queries must be addressed to the following: Tendercommittee@telecom.co.ls

1.2.2. Telecommunication Management Network (TMN)

TMN is defined in ITU recommendations M.3000 [4] series, with M.3010 [1] defining the principles for a telecommunications management network. TMN was defined in 1984 [4] as a concept to help public telecommunications operators [1] to manage the increasing centralized systems that support network control, management and supervision. The need for TMN as a standard was because networks with different types of equipment from different vendors or manufacturers and in different versions needed to be managed, hence there was a need for standardised interfaces and certain routines to be followed.

1.2.2.1. Why TMN?

According to recommendation M.3010 [1], TMN was adopted as a concept to "*support the management requirements of public telecommunications operators to plan, provision, install maintain, operate and administer telecommunications networks and services*". In addition to providing management functions, recommendation M.3010 [1] states that TMN also offers communications to another TMN or TMN-like networks. In summary M.3010 [1] states that "*the basic concept behind TMN is to provide an organized architecture to achieve the interconnection between various types of OSSs and/or telecommunications equipment for the exchange of management information using agreed architecture with standardised interfaces including protocols and messages*". The following terms are defined in M.3010 [1] as follows:

a) Management - " *a set of capabilities to allow for the exchange and processing of management information to assist PTOs in conducting their business efficiently*";
b) Telecommunications network – assumed to consist of both digital and analogue telecommunications equipment and associated support equipment;
c) Telecommunications Service – consists of a range of capabilities provided to customers.

1.2.2.2. Relationship of TMN to a Telecommunications Network

From [4], TMN is viewed as a model for operation and maintenance of telecommunications networks with the following objectives:

a) Functionality in a multi-vendor environment;
b) Optimization of network functionality.

These objectives come about due to the fact that most public telecommunications networks are huge and complex, ranging up to several network elements that need to be monitored. Network elements may be from different vendors and examples include [1]: transmission systems; switching systems; multiplexers; signalling terminals; front-end processors; mainframes; cluster controllers; file servers; databases; etc. Since its main objective is to manage the telecommunications network, a TMN is a separate network interfaced to the telecommunications network, which it manages and all the network equipments, which are managed are referred to as network elements. The need

for TMN to interface with the telecommunications network is to facilitate the sending and/or receiving of management information to/from network elements or other TMNs. Figure 1.2.1, shows the relationship of TMN and the telecommunications network.

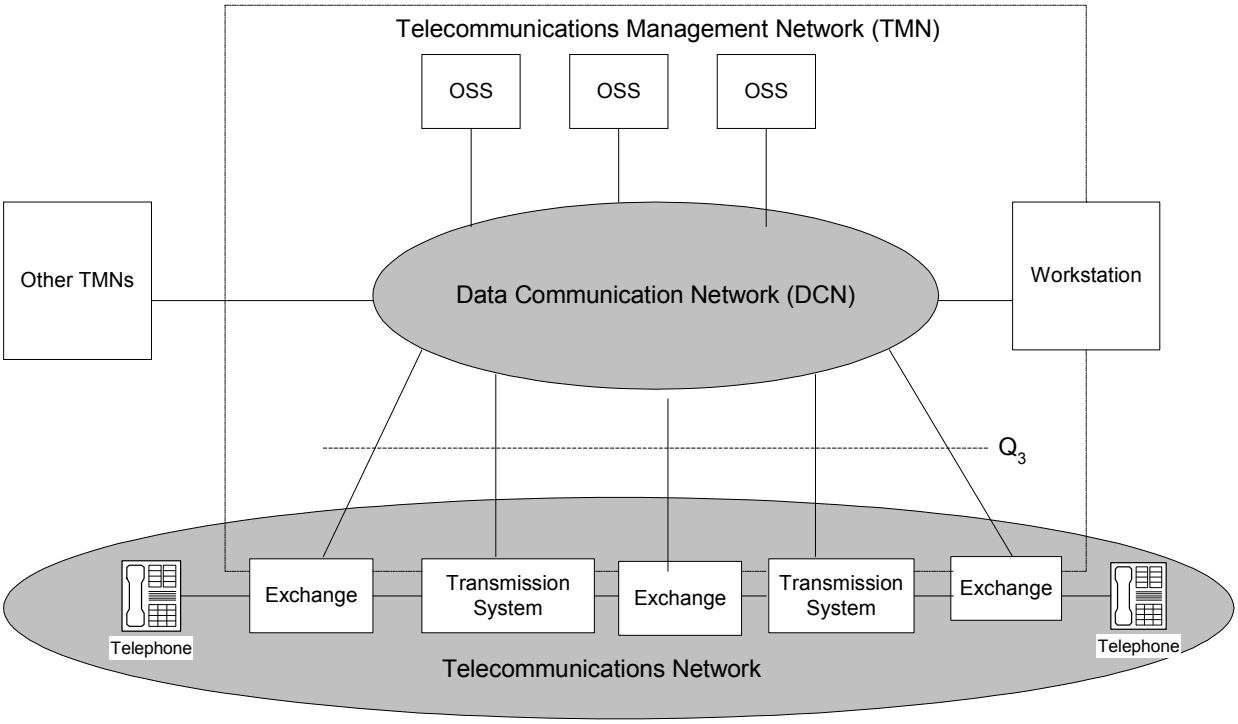

Figure 1.2.1. [1, 4, 6, 8] shows the relationship of TMN to the telecomms network

As seen form figure 1.2.1, OSS communicates with the network elements (exchanges and transmission systems) through data communication network (DCN), which is connected to the network elements via the Q_3 interface. This can be simplified into figure 1.2.2, showing the layered architecture in (a) and network model in (b).

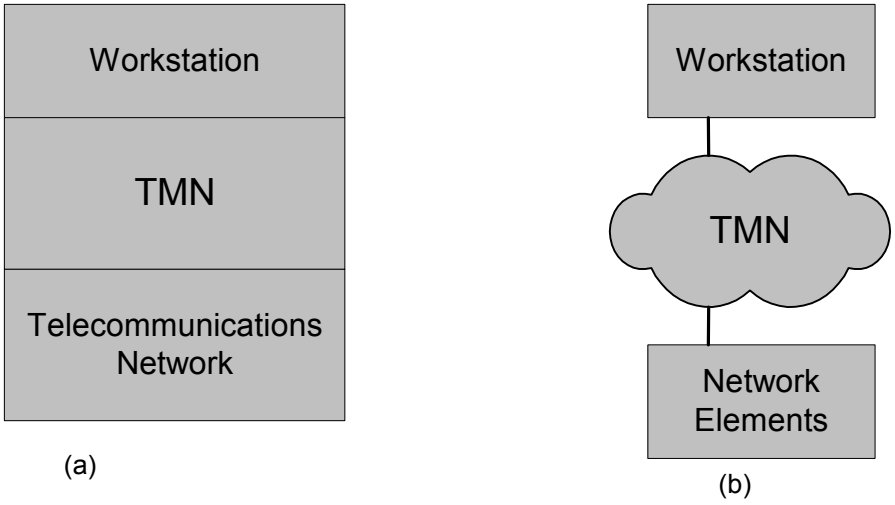

Figure 1.2.2, shows a simplified version of TMN relationship with telecommunication network

1.2.3. TMN Models

Several models of TMN have been identified in [1, 4, 8], in order to simplify the adoption of TMN, these models include:

a) Functional Model;
b) Reference Points;
c) Physical Model;
d) Management Layer Model.

1.2.3.1. TMN Functional Model

Functional model for TMN has been described in [1, 4, 8] to be the functional blocks that provide functions needed in TMN. Functional blocks are defined as entities that perform a certain management function. Reference points separate functional blocks, and the functional architecture is shown in figure 1.2.3.

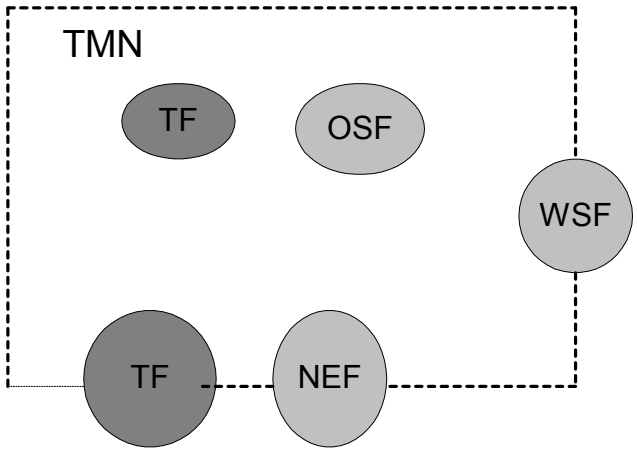

Figure 1.2.3, [1, 6], shows TMN Functional Architecture

From figure 1.2.3, there are four key functional blocks in TMN as follows [1, 4]:

a) OSF Block – handles the operations support programs used by the operators, by processing information related to the telecommunications management for the purpose of monitoring, coordinating and/or controlling telecommunications functions including management functions.
b) NEF Block – any functional block which communicates with the TMN for the purpose of being monitored and/or controlled, and they usually handle switching and transport processes.
c) Workstation Function (WSF) Block – handles TMN user terminals by providing means to interpret TMN information for the human user and vice versa.
d) Transformation Function (TF) Block – connects two functional entities with incompatible communication mechanisms, either protocols or information models.

1.2.3.2. Reference Points

"*Reference points define service boundaries between two management function blocks and identify the management information passing between functional blocks*" [8]. There are five (5) reference classes [1, 8] as follows:

a) Q Class – defines communications between OSS and NEs, and consists of Q_3, which defines communications between DCN and NEs as illustrated in figure 1.2.1. The Q interface is further divided into two parts [4] namely:
   - *Information model* – describes how functions in network elements are controlled and supervised. Information about managed objects (signaling terminals, etc) and their relationships with each other are contained in the database called management information base (MIB);
   - *Communication Protocols* – two protocols are supported by the Q interface namely [4]: CMIP – a transaction-oriented protocol suitable for transfer of alarm information and changes to subscriber data; FTAM – used for transfer of large amounts of data (files) for example, charging information and statistics.

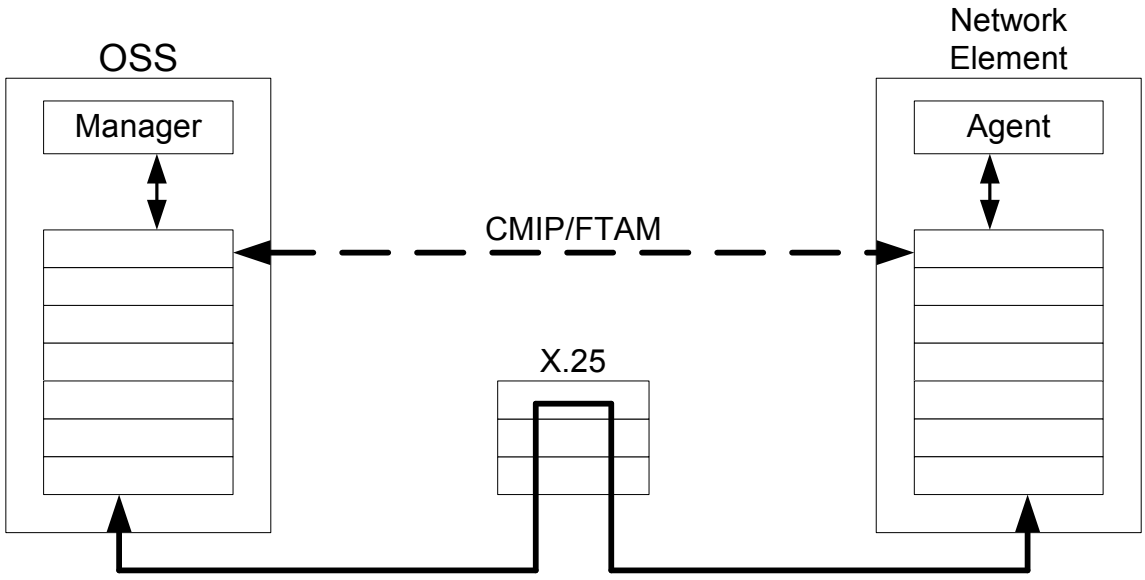

Figure 1.2.4 [4], shows communications protocols in TMN

b) F Class – located between WSF and OSF blocks.
c) X Class – located between OSF blocks in different TMNs.
d) G Class – a non-TMN point located between the human users and the WSF.
e) M Class – non-TMN point located between the TF and non-TMN managed entities or managed entities that do not conform to TMN recommendations.

Exercise: *Draw the TMN functional architecture with all the reference points included.*

1.2.3.3. TMN Management Layer Model

This model defines the TMN management functions into logical management layers, hence why it's sometimes referred to as TMN logical layered architecture (LLA) [1, 8]. This model is also referred to as a "*side view*" of network management [4]. There are five layers in this model [1, 4, 7, 8] namely:

a) Business Management – describes all functions related to business aspects; to analyze trends and quality issues, for example or to provide a basis for financial reports. X reference points are not supported at this layer in order to prevent access to its functionality and remain proprietary. And has four principal roles as follows [1]:

   - Supporting the decision-making process for the optimal investment and use of new telecommunications resources.
   - Supporting the management of OA&M related budget.
   - Supporting the supply and demand of OA&M related manpower.
   - Maintaining aggregate data about the total enterprise.

b) Service Management – describes functions for the handling of services in the network: definition, administration and charging of services. It's also responsible for the contractual aspects of services that are provided to customers and has the following four (4) principal roles [1]:

   - Customer facing and interfacing with other PTOs
   - Interaction with service providers
   - Maintaining statistical data
   - Interaction between services.

c) Network Management – describes functions for distribution of network resources; configuration, control and supervision of network functionality; and has the following five (5) principal roles [1]:

   - The control and coordination of the network view of all network elements within its scope or domain
   - The provision or modification of network capabilities for the support of services to customers
   - The maintenance of network capabilities
   - Maintaining statistical log and other data about the network and interact with the service manager layer on performance, usage, availability, etc
   - The network OSFs may manage the relationships (e.g. connectivity) between NEFs.

d) Element Management – contains all functions for handling individual network elements, including alarm management, handling of information, backup,

logging and maintenance of hardware and software, with the following three (3) principal roles [1]:

- Control and coordination of a subset of network elements on an individual NEF basis
- Control and coordination of a subset of network elements on collective basis
- Maintaining statistical, log and other data about elements within its scope of control.

e) Network Element Layer – "*the ultimate destination of TMN and does not have OS associated*" [8].

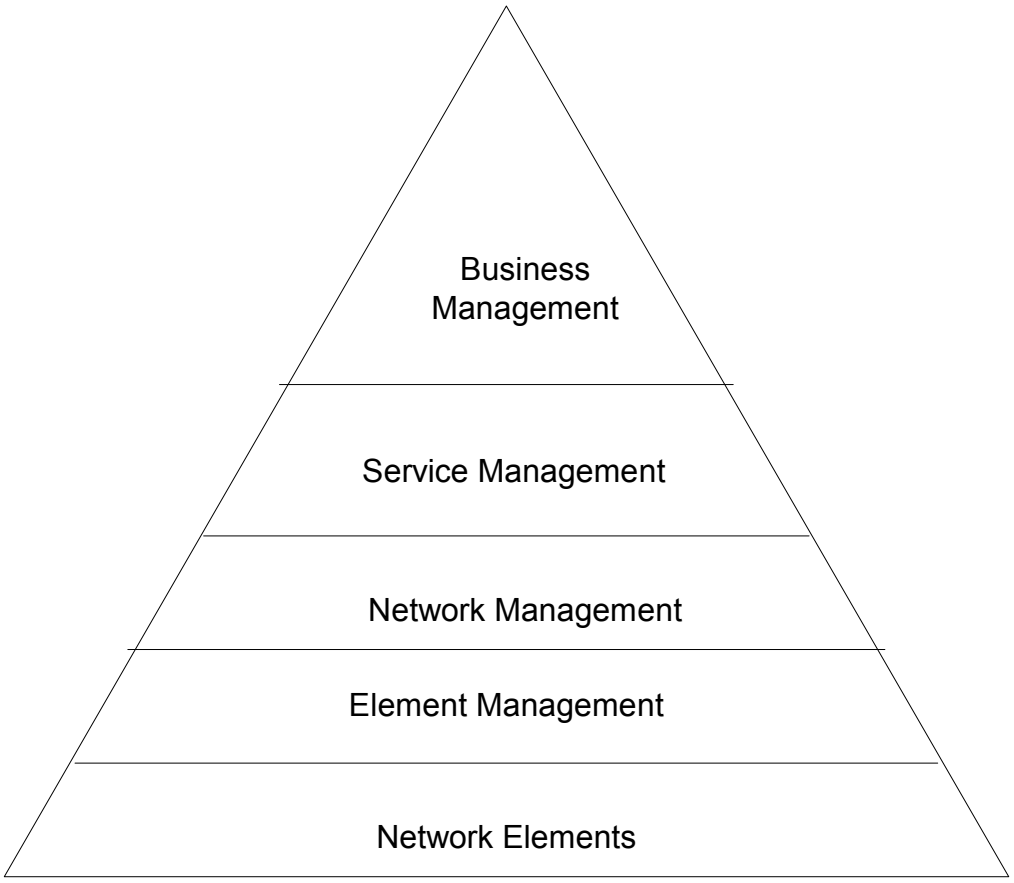

Figure 1.2.5, [1, 4, 6, 7, 16], shows Management Layer Model for TMN

However in some references [4, 16], this model is shown as only four (4) layers, with the last network element layer not shown.

1.2.3.4. TMN Physical Model

TMN physical model, figure 1.2.6., shows the physical (tangible) components which house functions identified in the TMN functional model, together with physical interfaces, discussed under TMN reference points.

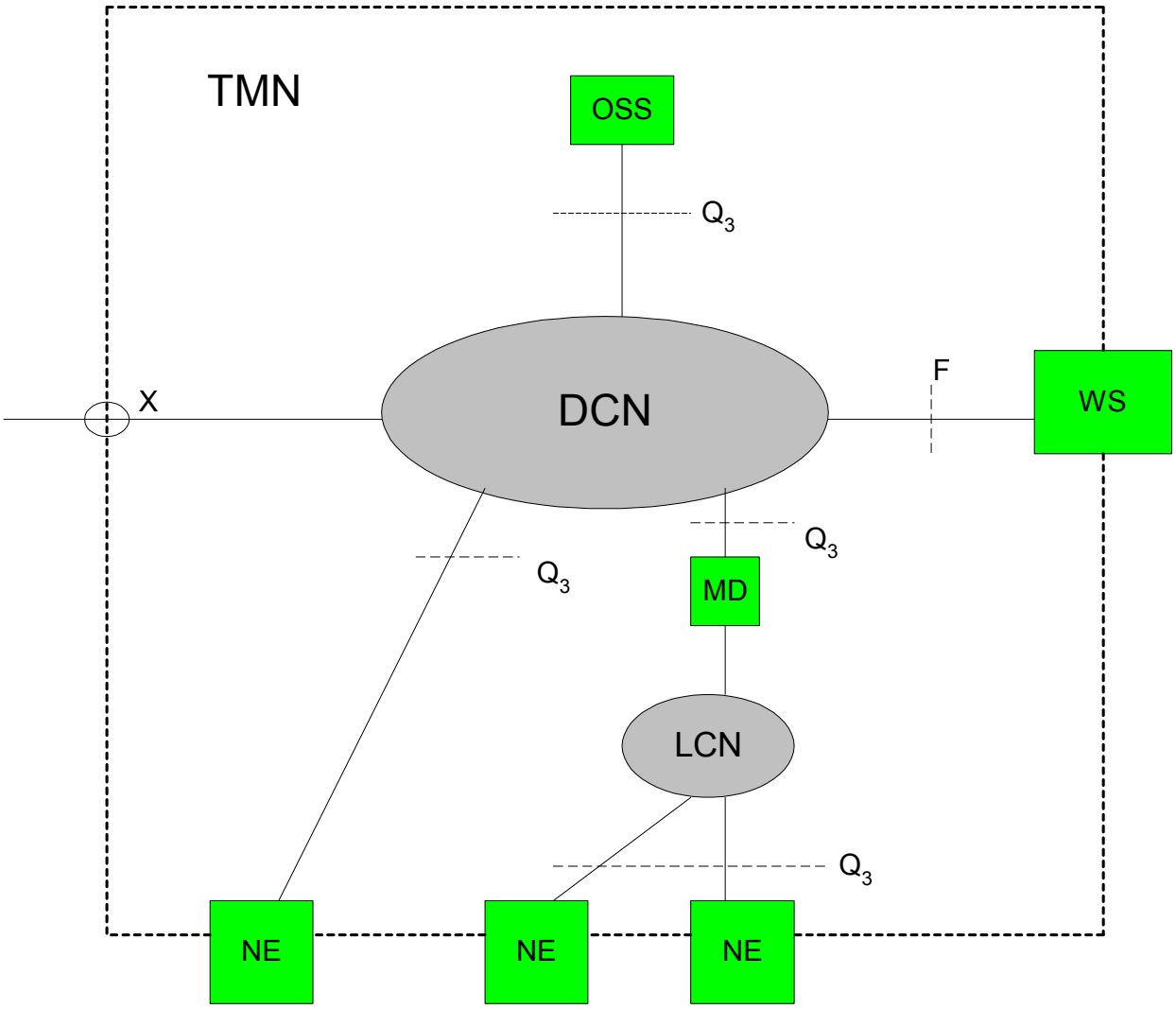

Figure 1.2.6, adapted from [1, 4], shows TMN Physical Architecture

From figure 1.2.6, the following physical blocks are identified as follows [1, 4]:

a) OSS – key TMN systems that perform the OSF and are connected to NEs through DCN, which in most cases is a packet-switched network either x.25 or frame relay network.
b) NE – TMN systems that perform NEF and include such network devices as exchanges, transmission systems, which are actually managed by TMN.
c) Workstation – TMN system that performs the WSF and translate information for the human operator. This workstation provides the human interface for TMN

functions, i.e. management information is represented in the way that humans can understand.

d) Mediation device (MD) – provides transformation between TMN physical blocks that incorporate incompatible communication mechanisms. In addition the MD concentrates, reduces and stores data. There are two types of MDs namely [1]:

   - QMD – supports connections and conversions within a single TMN
   - XMD – supports connections and conversions of OSSs in different TMNs.

e) Data Communications Network (DCN) – a supporting network that provides paths for information flow among the TMN physical blocks. It may be a local or wide-area network, which is technology-independent. DCN acts at the transport layer of OSI and services the four lower layers of OSI reference model.

f) Local Communications Network (LCN) – instead of having regenerators for OSI transport functions provided by DCN, simpler network elements may be connected over the local networks provided by either SDH or PDH overhead capacity [4].

1.2.4. TMN Management Functional Areas

Section 1.2.3.3, discusses TMN management layers, referred to as the "*side-view*" of network management. From this side-view, each layer is subdivided into five (5) functional areas, viewed as a "*plane view*" [4] of network management. These functional areas form what is referred to as TMN FCAPS model [7] as an arbitration of the five areas namely: ***F***ault (F), ***C***onfiguration (C), ***A***ccounting (A), ***P***erformance (P) and ***S***ecurity (S). There is a full ITU-T recommendation for TMN FCAPS model in the form of a 110-paged M.3400 recommendation [2], titled "TMN Management Functions". These five areas are summarized from [2, 3, 4, 7, 8, 9, 11, 16] as follows:

a) Fault Management – deals with a set of functions, which enables the detection, isolation and correction of faults in the telecommunications network. The key component of fault management is RAS – ***r***eliability, ***a***vailability and ***s***urvivability measurements. These functions are grouped as follows: RAS quality assurance, alarm handling and surveillance, fault detection and localization, fault correction, testing, logging and reporting; and network recovery.

b) Configuration Management – deals with a set of functions, which enables network planning and engineering installation of network equipment, service planning and negotiation, network provisioning, backup and restore strategies, configuration of network capability, etc.

c) Accounting Management – deals with a set of functions that enable measurement of network services in order to determine prices that customers can pay based on their network usage. These functions are grouped as usage measurements, tariffing/pricing, collections and finance. In short accounting management deals

with the collection, buffering and delivery of charging and accounting information.

d) Performance Management – monitors statistics about performance of the telecommunications network and offered services in order to maintain the levels agreed with uses in SLAs. The overall behavior of the network is managed here by gathering, collecting and analyzing statistical data, for the purpose of monitoring and correcting the behavior of the network so as to maintain the high quality of service.
e) Security Management – monitors access to the network and grants only authorized users and protects against the intrusion from the public telecommunications network. It also handles simultaneous use of an OSS, and detects, isolates and prevents all security violations in order to maintain privacy and management information integrity. ITU-T has provided a 25-paged document, recommendation M.3016 [3], titled "TMN Security Overview", which deals with TMN security in addition to the portion in Recommendation M.3400 [2].

1.3. OSI Management and Internet Management

1.3.1. Introduction

According to recommendation X.700 [25], management is related to all activities which monitor and control resources and their use. In open systems resources include [25]:

a) Storage
b) Processing
c) Interconnection capabilities

OSI management [6, 25] standardization only cover those resources, which provide interconnection capabilities between open systems and the communications concerning their management; with human beings or automated processes expected to be responsible for managing the OSI environment (OSIE). OSI management is a combined effort of ISO and ITU-T [6], and both organizations publish the same standards with ITU-T X.700 [25] and ISO 7498/4 detailing OSI management framework. According to [5], a network manager has to monitor and control the hardware and software that comprise an internet (any data network including the global Internet). However, there are two major problems in managing the internet as follows [5]:

a) The internet contains hardware and software from different vendors, there is a higher need for compatibility
b) Most internets are large e.g. the global Internet; thus diagnosing a problem is very complex.

Due to this complexity, there are different types of failures: other failures may be very easy to troubleshoot and correct, e.g. power failure of a LAN switch; other failures may be partial (intermittent failures) – which normally remain hidden, yet affect performance of the entire network. Examples [5]: a router that incorrectly routes a few packets, while the majority are routed correctly; an interface card that infrequently corrupts bits.

1.3.2. OSI Management

ITU-T recommendation X.700 [25], defines OSI management as "*the facilities or activities to control, coordinate and monitor the resources which allow communications to take place in the OSI environment*". These activities relate to the means by which:

a) A real open system obtains information to enable the supervision and control of its communications resources; and
b) Real open systems cooperate to supervise and control the OSI environment.

In an OSI environment, there is the OSI management environment, which is a subset of OSIE and deals with tools and services that monitor, control and coordinate interconnection activities. In addition, the OSIME includes [25]:

a) The capability for managers to gather information
b) The capability for managers to exercise control on the information
c) Capability to maintain an awareness of the status of resources in the OSIE
d) Capability to report on the status of resources in the OSIE.

OSI management is defined in the OSI management framework [6, 25], standard and in this course only the functional areas, exchange of management information are discussed in the following sections.

1.3.3. OSI Management Functional Areas

Like most management architectures, OSI management also covers the five (5) functional areas of "FCAPS" [6, 9, 10, 11, 25], which are briefly discussed in the next sections.

1.3.3.1. Fault Management (F)

According to recommendation X.700 [25], [6], and [10], fault management includes all activities related to fault detection, isolation and correction of abnormal operation of the OSI environment. Such functions or activities include to:

a) Maintain and examine error logs
b) Accept and act upon error detection notifications
c) Trace and identify faults
d) Carry out sequences of diagnostic tests
e) Correct faults.

1.3.3.2. Configuration Management (C)

Configuration management is mainly concerned with the assignment of names, addresses or any useful ID's to all devices within the OSI environment, and consists of a set of facilities, which [6]:

a) Records the current configuration
b) Records changes in the configuration
c) Identifies network components (gives addresses to service access points and network devices)
d) Initializes and closes down network systems
e) Changes network parameters (e.g. routing tables)

1.3.3.3. Accounting Management (A)

Recommendation X.700 [25], classify all activities, which enable charges and costs to be established for the use of resources in the OSIE, so that users can be billed accordingly, under accounting management. Accounting management functions includes functions to:

a) Inform users of costs incurred or resources consumed;

b) Enable accounting limits to be set and tariff schedules to be associated with the use of resources; and
c) Enable costs to be combined where multiple resources are invoked to achieve a given communication objective.

1.3.3.4. Performance Management (P)

Performance management ensures that the network functions according to agreed levels by monitoring the statistics about its behavior and the level of customer satisfaction, and includes functions to [25]:

a) Gather statistical information;
b) Maintain and examine logs of system state histories;
c) Determine system performance under natural and artificial conditions; and
d) Alter system modes of operation for the purpose of conducting performance management activities.

1.3.3.5. Security Management (S)

Security management covers all those activities which allow the manager to control access to the network, deny unauthorized access, maintain network and services, integrity and privacy; control user behavior; maintain firewalls; create security policies and logs; etc.

1.3.4. Exchange of Management Information

OSI management classifies three (3) types of information exchange as follows [6, 25]:

a) Systems management
b) Layer management
c) Layer operation

1.3.4.1. Systems Management

According to [6], the definition of "systems management" as found in the OSI Reference Model, distinguishes between two different properties:

a) Systems management is related to the management of OSI resources and their status across all layers of the OSI architecture (*what is being managed)*
b) Protocols for systems management reside in the application layer (*exchange of management information*).

In OSI management framework, the key concern is how to exchange management information, relating to the monitoring, control and coordination resources in open systems. In this exchange application layer of OSI RM is used and systems management application entities (SMAEs) are introduced, as entities which reside in the application layer and realize the communications aspect of the systems management functions, as shown in figure 1.3.1. Systems management protocols are application layer protocols.

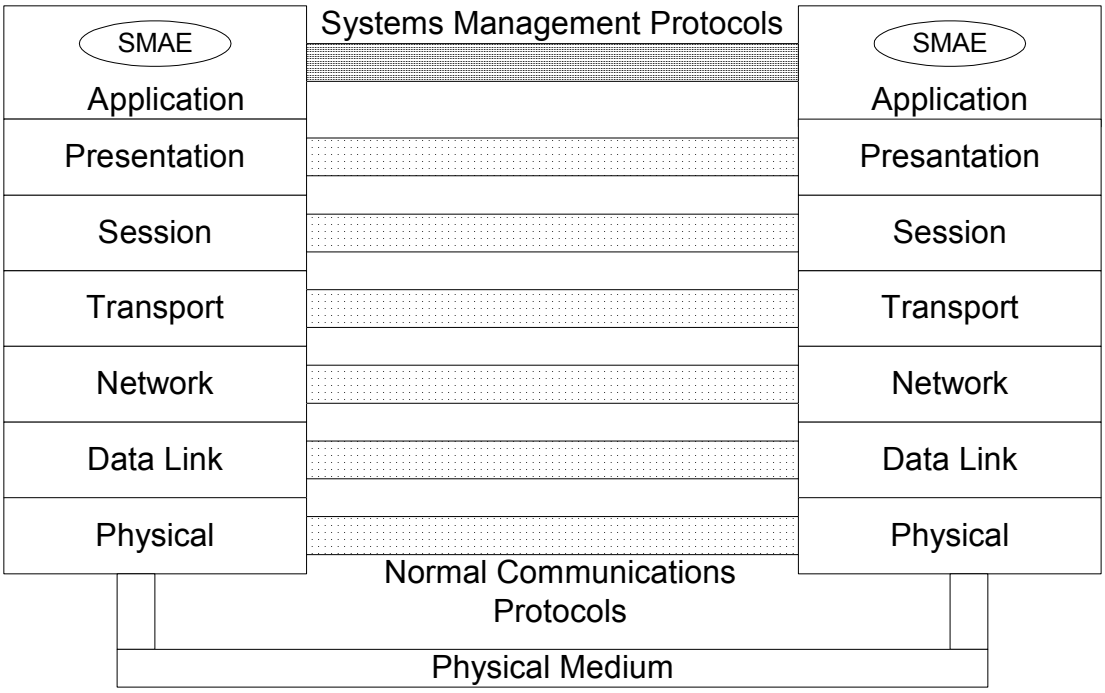

Figure 1.3.1, Adapted from [6, 25], shows systems management information exchange

1.3.4.2. Layer Management

Instead of using the presentation layer for management information, as in systems management, layer management relies on the layer immediately below and all those below it to transport the management information. With layer management, the monitoring, control and coordination of layer-managed objects is possible. An example is shown in figure 1.3.2, which shows the typical example of routing information, which occurs at layer 3, and is inefficient to involve all the upper layers; especially the presentation layer, which does not support broadcast capabilities, yet routing information needs to be broadcasted.

Other examples include: bridge PDUs, configuration PDUs from network entities and Hello PDUs from routers [6]. "*N-layer management protocols are supported by protocols of the layers (N-1) and below*" [25]. However, layer management is only used when special requirements dictate that systems management protocols are inappropriate or when they are not available.

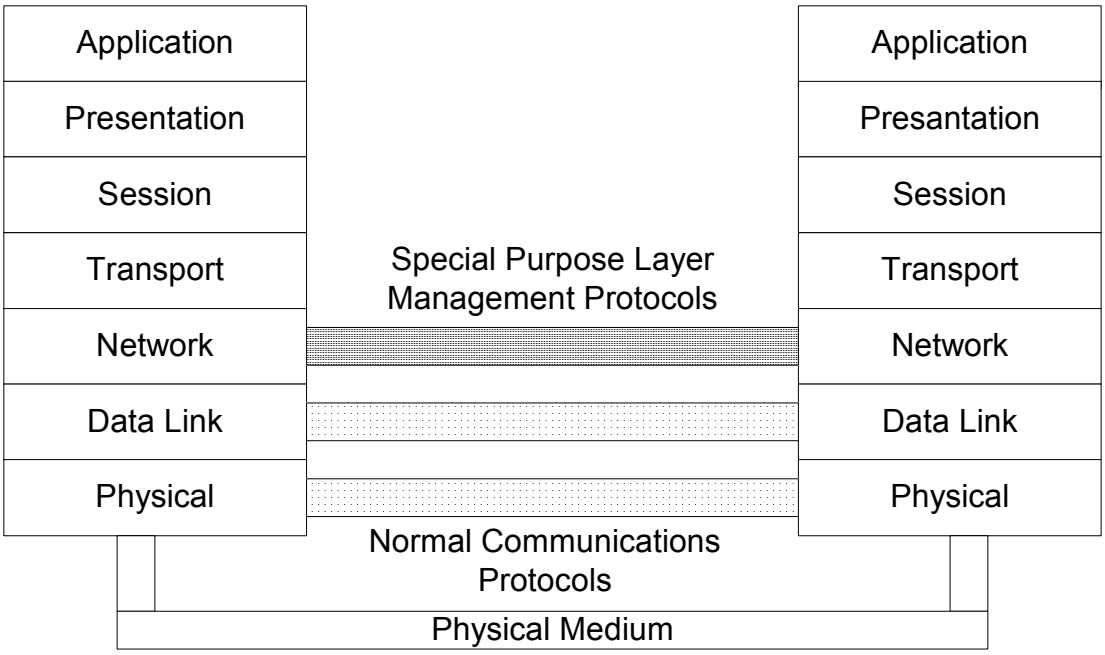

Figure 1.3.2, [6, 25], shows layer management exchange

1.3.4.3. Layer Operation

Layer operation is the "*set of facilities which monitor, control and manage a single instance of communication*" [6, 25]; and carries management information as part of a normal layer protocol and uses the same concept as layer management. Examples: passing of charging information in an X.25 clear packet or an X.25 reset command. There must be a clear distinction between management information carried by the protocol and information for other purposes.

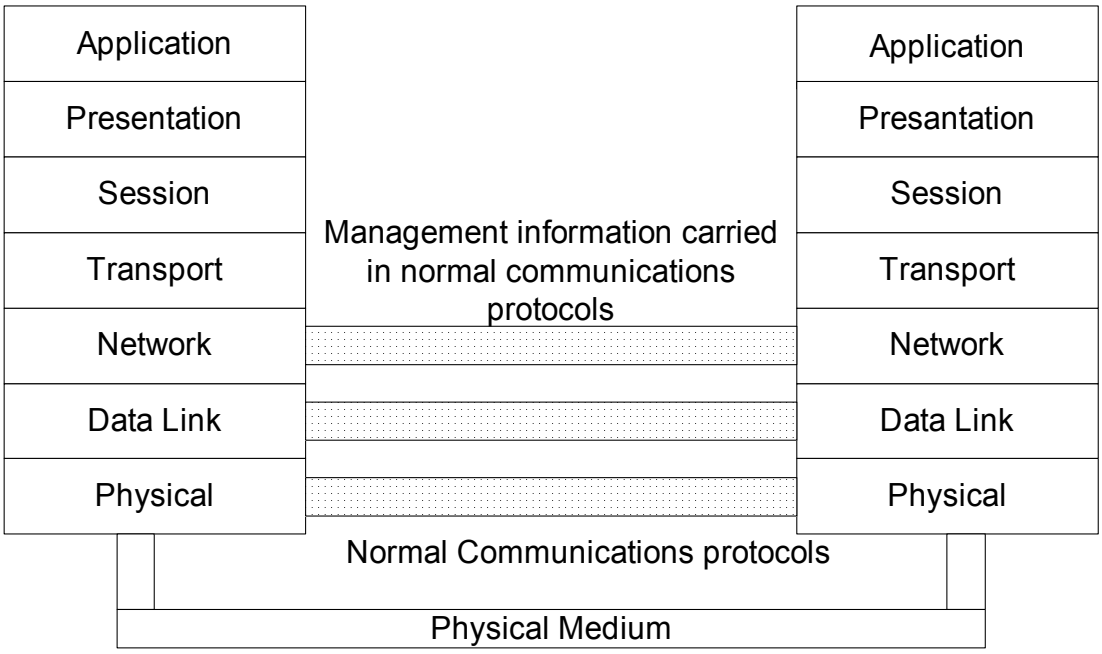

Figure 1.3.3, [6, 25], shows layer operation

1.3.5. Managed objects, Management information and MIB

OSI management is developed by the International Standards Organization (ISO) and has been modeled in four (4) different ways as follows:

a) **Organizational** – concerned with the actual devices or equipment used in the OSI management environment. These devices are the network management station (NMS) commonly called a "manager", which refers to systems responsible for gathering management information about the managed network elements; and the network agents, commonly called just "agents". An agent is the software installed in the managed device that helps the device to be managed, and such devices include: PCs, IP phones, servers, IP-PABXs, routers, switches, gateways, etc. The organizational model also looks at the relationships between managers (NMS) and agents, and these relations usually follow a client/server model but occasionally agents may send commands to the manager, without the manager first requesting their status. In [6], a managed object is defined as: "*those data processing and data communications resources (whether OSI resources or not) that may be managed through the use of an OSI management protocol*". Each managed object ("*logical representation of the real physical entity on the network*") [18], has attributes and a behavior; receives operations from the manager; and sends out notifications to the manager (NMS).
b) **Information model** – deals with the structure of the management information (SMI). SMI defines the syntax and semantics of management information, stored in the database. Management information is defined as "*information associated*

with a managed object that is operated on by the OSI management protocol to control and monitor that object" [6]. The database, which stores the management information, is referred to as the management information base (MIB) [4, 6]. In addition to this information, MIB also contains the managed objects themselves. As an example, the information about the router's identification (IP address or name), daily statistics, and correct packets sent or received, corrupted packets, etc, are all stored as MIB. The managed objects reside in different layers of the OSI-RM, so, each layer has to know how to handle information regarding that device. As an example, a router operates at layer 3, switch at layer 2, NIC at layer 2, and a gateway at all layers.

c) **Communication Model –** discussed under section 1.3.4, deals with the exchange of management information, in the form of:

- Systems Management
- Layer Management
- Layer Operation

d) **Functional Model –** discussed under section 1.3.3, deals with the "FCAPS" functional areas.

1.3.6. Internet Management Standard

The Internet management standard developed by IETF in late 1980's [10] and adopted as TCP/IP standard in 1989, is the Simple Network Management Protocol (SNMP) [5, 6, 8, 10, 18]. Since it has been standardized for TCI/IP, it has also been referred to as "TCP/IP Management Approach" [6]. SNMP originated from simple gateway monitoring protocol (SGMP), which was a huge success in managing intermediate systems (gateways), so the extension to include more capabilities and management of end-systems, resulted in SNMP [6]. The main aim of SNMP is for management of IP-based networks and is the dominant framework in the computing industry [10], and consists of a protocol (for transfer of management information), a database structure specification and a set of data objects. Because of the fact that it contains a protocol, SNMP is viewed as an application layer protocol for the exchange of management information between NMS and agents, and is built over the connectionless transport protocol called user datagram protocol (UDP) [6]. UDP is however unreliable, with the possibility of losing user data and this as well can affect management information. But, the use of UDP has been deliberate [6], mainly because even during repeated failures, it's possible to still exchange some part of management information. Had connection-oriented transport been used, there would be no exchange, since it is all or nothing mechanism; whilst UDP is the best-effort approach. Another concern is that with connection-less UDP, the manager has to keep polling devices (agents), so as to determine if they are still operational, however if connection-oriented protocols were used this would not be necessary. UDP also has a characteristic that packets cannot

exceed a certain size and SNMP obeys this by ensuring that if the maximize size is exceeded; no information will be exchanged at all.

1.3.6.1. SNMP Framework

SNMP framework, shown as figure 1.3.4, consists of four (4) elements namely [10]:

a) Management Station (NMS)
b) Managed Objects (Agents)
c) Management Information Base – database
d) Network Management Protocol

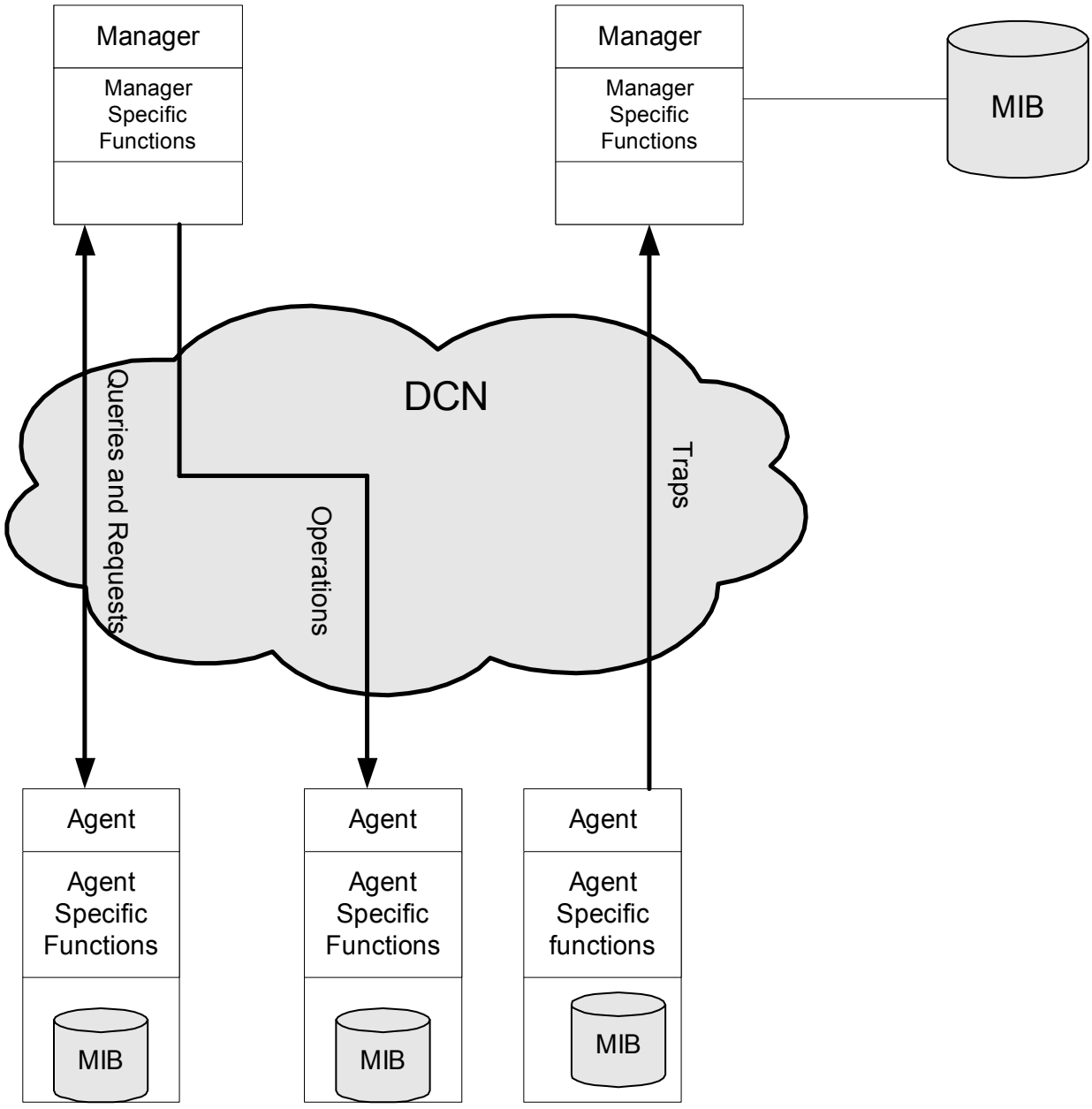

Figure 1.3.4, shows SNMPFramework, with local MIBs for each managed object

From figure 1.3.4, the management station (NMS) is normally a workstation equipped with a network management application (NMA), e.g. HP Openview, SNMPv2c; which includes a user interface for human operators to actually interact with the manager (NMS) and agents, though several commands. The agents are the managed objects, which include: PCs, routers, bridges, servers, switches, gateways; and are all equipped with SNMP client software, so they can be managed. NMS send requests for information and action to the agents, which have to respond to such requests. In addition, agents themselves may send notifications about their status to the NMS. Each agent's management information is stored in that agent's local MIB. To monitor the

agents, the NMS retrieves the values from the agent's MIB. The communications between NMS and agents is carried over the data communications network and is through UDP ports 161 and 162.

1.3.6.2. SNMP Messages

The communications between NMS and the agent relies on the exchange of three (3) types of messages as follows [6, 8]:

a) *Get* – used to retrieve management information (value of MIB objects) from the agent, which is expected to respond.
   - GetRequest
   - GetNextRequest
   - GetBulkRequest – only available from SNMP v2

b) *Set* – used by the NMS to store (change) management information (or to set the value of MIB objects) at the agent.
   - SetRequest

c) *Trap* – unsolicited notification from the agent to the NMS about significant events, such as link status. The trap reception is not confirmed by the NMS.

Once the agent has received either the Get or Set commands, it has to respond with a Response PDU, which carries the requested information or indicates failure of the previous request.

1.3.6.3. SNMP v1 Weaknesses

The SNMP v1 protocol had several weaknesses including [6, 10, 18]:

a) Access control such as "Community Strings" (passwords) were transmitted in clear text, i.e. there were no security features;
b) Transfer of table data required multiple small operations – which resulted in reduced performance;
c) Limited trap types, with "urgent trap message", the only command which could be initiated by the agent.

1.3.6.4. SNMP v2

SNMP v2 came as an improvement to SNMP v1, but ended up being more popular than SNMP v1 [10], and unfortunately more complex than SNMP v1 [6]. With SNMP, the following improvements were introduced [6, 8, 10, 18]:

a) GetBulkRequest – gets large amounts of data (e.g. all data in a large table) in one single operation. This improved performance of SNMP as many GetRequests and GetNextRequests were avoided;
b) 64-bit counters to the MIB – with the increasing speeds of Ethernets (now in Gbps ranges), counters easily rolled over in SNMP v1;
c) PDU format was also changed in version2 and more trap messages were added;

d) Introduction of hierarchical management structure with top-level and intermediate-level managers;
e) More efficient information retrieval.

1.3.6.4. SNMP v3

The problem of security was not addressed in version 2, so, it was passed over to version 3 [8]. In SNMP v3, fully-fledged security mechanisms were added, which support concurrent existence of multiple security models, and provides encryption of passwords. In addition, new terminology, more performance measurement matrixes and alarm MIB's were introduced in version 3. [8].

1.3.7. Remote Monitoring

Remote monitoring (RMON) [8, 18], extends the capabilities of SNMP to large IP-based internetworks and overcomes some of the limitations of SNMP, though it still relies on the underlying SNMP. This extension of capabilities is made possible by managing subnetworks as opposed to individual managed objects in SNMP. So, with RMON, there is one monitor per subnet, which is a dedicated management entity, called a "probe" or a remote monitor. With RMON, a "*probe monitors the health and behavior of a segment of a network, reducing the burden on the management station*" [8]. RMON is simply a special-purpose MIB, defined in IETF RFCs and gathers statistics by analyzing every frame on a network segment.

SNMP vs. RMON Illustration [18]

"To put these protocols in perspective, assume you are a city planner and you need to monitor traffic at various intersections throughout the city. One way to do this is to have people (called agents) stationed at important intersections to gather traffic information. These agents have portable phones. As they collect traffic information, they write it down. Also part of this scheme are data entry clerks at a central office. They call the agents on a continuous basis to collect the information that agents have obtained and enter it in a computer for future analysis.

The only problem with this technique is the overhead of making all those phone calls. A more efficient method would be to give the agents their own personal computers and have them enter the traffic data as it occurs, then transfer that data to the central office on a regular basis or upon the request of a manager who needs it.

Of course, the less efficient model described above is analogous to traditional SNMP data collection while the more efficient method is related to RMON".

In IETF RFCs, the following RMON goals are stated [8]:

a) Offline operations
b) Proactive monitoring
c) Problem detection and reporting for distributed LAN-based networks

d) Value-added data
e) Multiple managers support.

RMON framework consists of [8]:

a) Management station (same as in SNMP)
b) Set of RMON probes
c) Management protocol identical to the one used in the existing SNMP management systems.

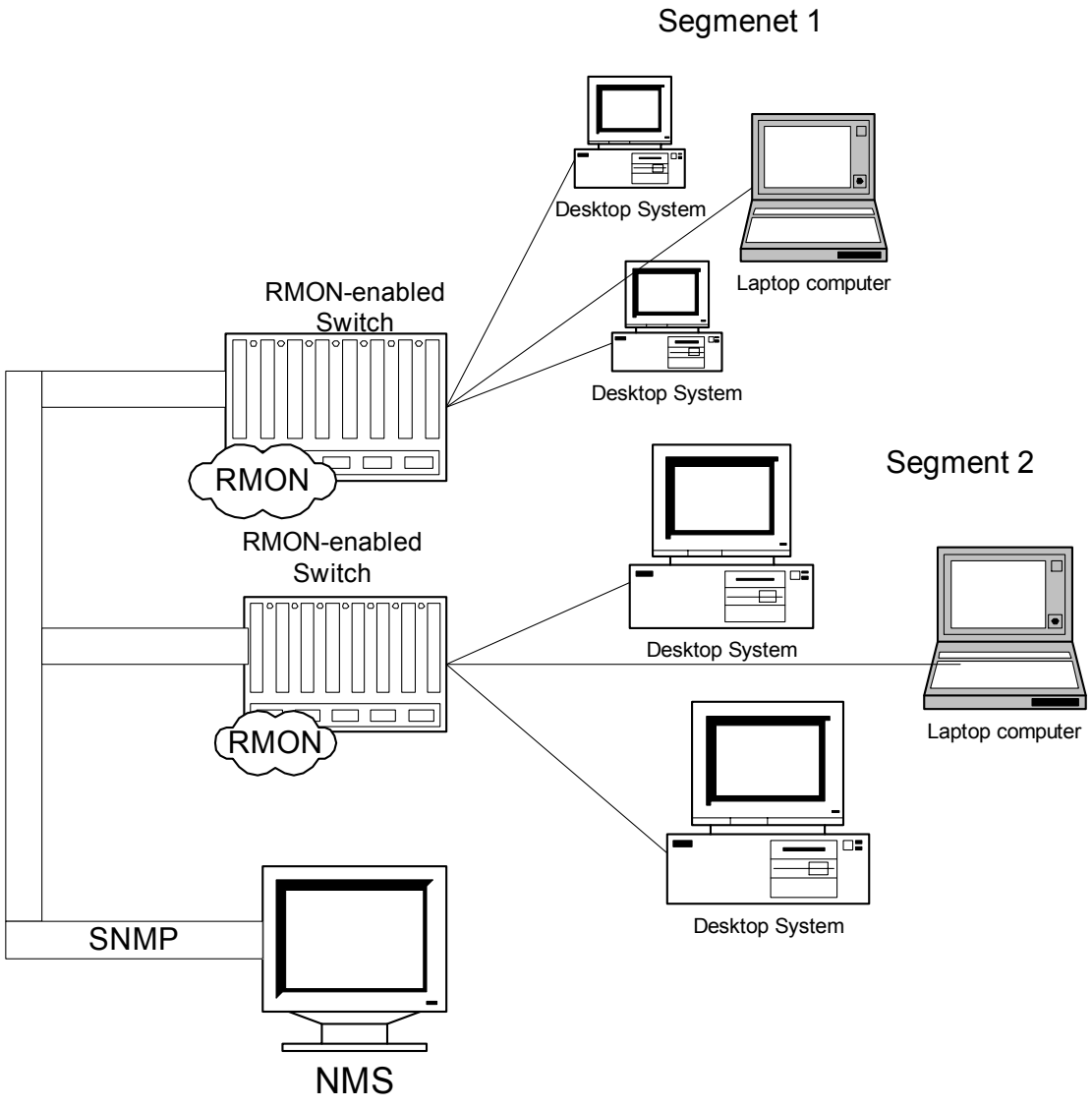

Figure 1.3.5, adapted from [18], shows RMON network configuration

RMON has different groups, which enable managers to get information related to certain activities only as follows [18]:

a) **Statistics –** Collects and accumulates LAN traffic statistics and errors;
b) **History –** Collects statistics at defined intervals for use in historical analysis;
c) **Alarms –** Provides alerts when predefined thresholds are exceeded;
d) **Host –** Collects information and provides statistics based on MAC (Medium Access Control) addresses;
e) **HostTopN –** Collects information about which hosts are transmitting the most traffic;
f) **Matrix –** Collects information about which devices are communicating with one another;
g) **Events –** Provides a way to trigger actions based on alarms;
h) **Packet Capture –** Provides a way to select the type of packets to collect;
i) **Filter –** Provides a way to view only selected packets when analyzing information

1.3.8. Common Management Information Protocol

CMIP [6, 10, 18], is the management protocol for OSI-based networks '6, 10, 18], which defines a management service, a protocol, a database and a set of data objects and is documented as ITU-T Recommendation X.711 or ISO/IEC Recommendation 9596 [6]. It was created for the monitoring, controlling and managing of heterogeneous networks (open systems). CMIP defines how to create common network management systems and is used by some telephone companies for public network management. Common Management Information Service (CMIS) [18] provides a way to share information in the CMIP environment, by defining services for accessing information about network elements (managed objects), controlling them, and receiving status reports from them. Both CMIP and SNMP define network management standards, but CMIP is richer in functionality, but has the following downfalls [18]:

a) Slow acceptance
b) Few CMIP products exist
c) Some of the supporting components have not been standardized.

Compared to SNMP, which is [18]:

a) Commonly used on corporate networks (TCP/IP networks),
b) Most popular network management protocol,
c) Well tested, and
d) Easy to implement.

1.4. Information Technology Infrastructure Library (ITIL)

1.4.1. Introduction

Sections 1.2 and 1.3 introduced TMN and OSI management based mainly on the hardware and systems point of view. But the networks are solely for the transmission of data, voice, video, etc; and are basically there to support services offered by IT to the business. IT is the most important factor in increasing business productivity and effectiveness with several services offered through IT. This makes IT the key component to most businesses, which want to gain an edge in the global competition. Businesses today are being transformed by both change and innovation. Innovation in IT improves the business as a whole and leads to companies stealing a match ahead of their competitors. All most all businesses today have an IT division or at least they may opt to outsource their IT division, but PC and other ICT infrastructure are used by all businesses, so, like it or not IT is here to stay. Other businesses are realizing this and are now: "*harnessing the power of IT to create value in a highly competitive market. Few businesses today do not rely on IT for at least one critical function*" [12]. All facilities offered by an IT department are viewed as "services" defined in [12] as: "*a set of related functions provided by IT systems in support of one or more business areas. This service can be made up of software, hardware and communication facilities, but the users perceive it as being a self contained, coherent entity*".

IT departments are not just required to offer and support IT services, but they must ensure that these services are of high quality, reliable and accurate. In order to achieve these, there must dedicated and focused infrastructure consisting of [12]:

a) Hardware
b) Software
c) Communications
d) Documentations
e) Skills (Personnel).

The management of this infrastructure in known as "service management" [12] or IT service management [13, 14] and is summarised in [12] as follows: "*services is aimed at providing services that facilitate the achievement of corporate objectives and business goals in a timely and cost effective manner*". ICT has become crucial in businesses, however several issues need to be solved before the greater benefits of ICT systems and services can be reaped by the business. These issues are outlined in [13] and include:

a) Demonstrating the business value of IT
b) Using IT to gain competitive advantage
c) Managing constant business and IT change
d) Reducing costs and TCO

e) Integrating and aligning IT and business goals
f) Etc.

In response to the need of effectively providing, supporting, and managing ICT and IT services, service management strategies were developed and ITIL is one of them. ITIL was developed by the Central Computing and Telecommunications Agency (CCTA) [9, 12, 16] in the 1980's. CCTA now part of the office of government commerce (OGC)'s goal is "*to improve business effectiveness and efficiency in the UK government using IT*". However CCTA realized that good management practices were needed to make government IT productive and useful. "*In the 1980's the CCTA realized that making the government effective and efficient through IT was going to take more than good software and hardware. There had to be good management to ensure that it was being used to the best advantage. With the assistance of recognized experts in IT management fields, the CCTA began to document what experience had taught were the best practices in the management of an IT infrastructure*" [12].

1.4.2. ITIL and ITIL Framework

The key aim of ITIL is to provide guidelines on how to provide quality It services to the organizations through the use of the four (4) P's [13], which are people (IT personnel), processes, products (tools and technology) and partners (suppliers, vendors, and outsourcing organizations). ITIL is a set of best practices or standards for IT service management [16] and is organized into sets of texts [16] or library of books [12], with each covering a different aspect of IT infrastructure management from the following [12, 13, 14, 15, 16]:

a) Service delivery
b) Service support
c) The business perspective
d) ICT infrastructure management
e) Security management
f) Applications management
g) Planning for the implementation of IT service management.

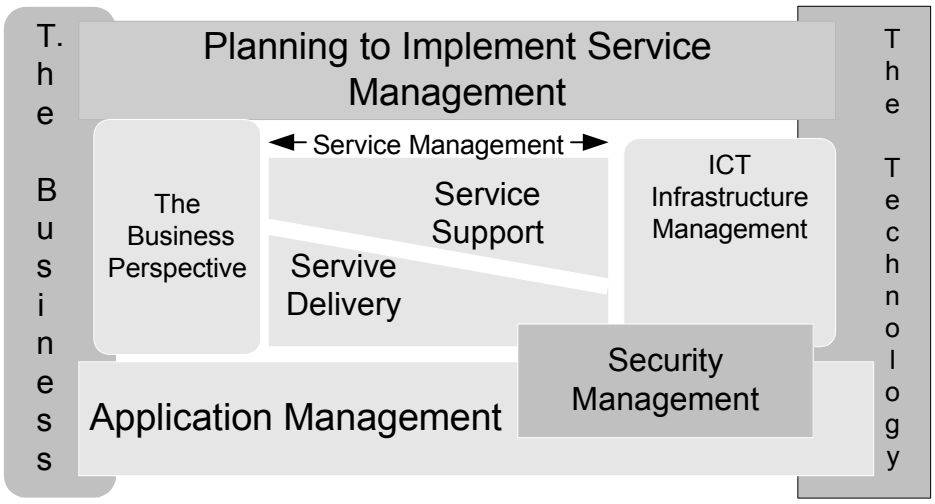

Fig 1.4.1, adapted from [13, 14] , shows the ITIL Framework

In addition to this ITIL aims to provide quality customer care and relationship management and "assists IT service provider organizations to improve IT efficiency and effectiveness whilst improving the overall quality of service to the business within imposed costs constraints" [13]. All areas addressed by ITIL are shown as a framework in figure 1.4.1 and each will be addressed briefly in section 1.4.3. Full details can be found in [12].

1.4.3. Service Management

Service management is the key part of ITIL [14] and is composed of two sections namely: service delivery and service support. As has been discussed, IT departments have to offer IT services to businesses, once the services are delivered, they have to be supported and managed to maintain the required level of performance, quality, reliability and availability. Both service delivery and support have several processes or functions as shown in figure 1.4.2.

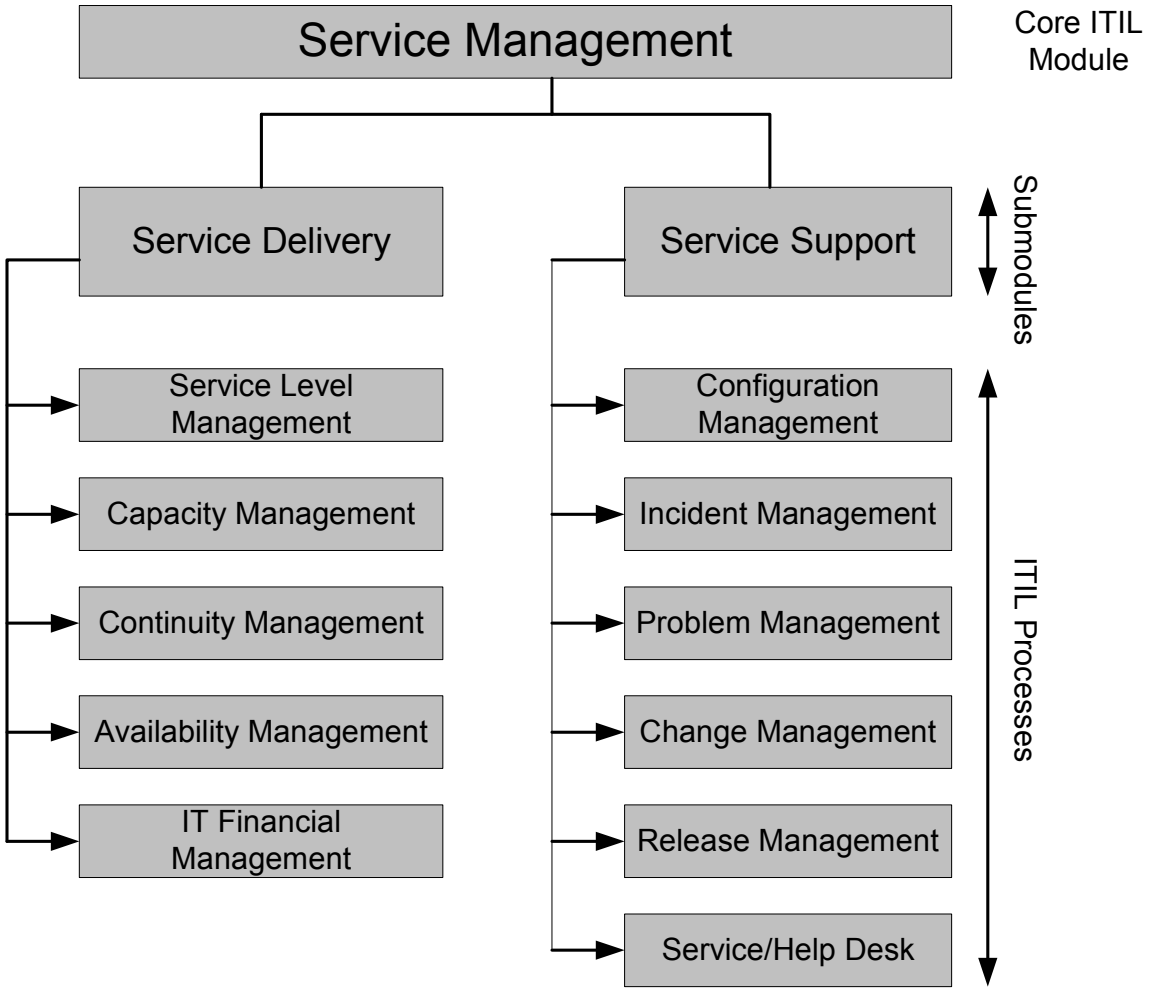

Figure 1.4.2, adapted from [12, 14, 16], shows ITIL processes that comprise Service Management

As shown from figure 1.4.2, service delivery has five functions or processes, which help in achieving its goals. "*Service delivery covers the processes required for the planning and delivery of quality IT services and looks at the longer term processes associated with improving the quality of IT services delivered*" [13].

1.4.4. Service Delivery

Before services can be used by the business, they have to be first planned and designed by the IT department, then they have to be delivered, once thorough testing and re-testing have been carried out. So, service delivery as a sub-module of service management "*covers the processes required for the planning and delivery of quality IT services and looks at the longer term processes associated with improving the quality of IT services delivered*" [13]. As shown from figure 1.4.2, service delivery is composed of five processes as follows [12, 13, 14, 15]:

a) **Service Level Management (SLM)** – in general SLM aims to manage the business-like relationships between the IT service user (herein called customer)

and the IT service department (herein called supplier). These relations are documented in the form of a contract between the two parties (supplier and customer) fully stipulating the user requirements, expectations and agreements with the supplier of the IT service. The agreements between the user and supplier are documented as service level agreements (SLA), and SLM ensures that SLAs are in place and "*monitors the actual supplied service levels to ensure that they conform to SLAs*" [14]. In addition SLM also negotiates and monitors the operational level agreements (OLA) between IT departments and their external suppliers or support teams. OLA documents agreements between IT departments and the suppliers in support of SLAs, i.e. for an IT department to meet its obligations to customers, their supplied equipment and systems must also be of high standards and be reliable. In summary SLM process negotiates, documents, agrees and monitors SLA and OLA.

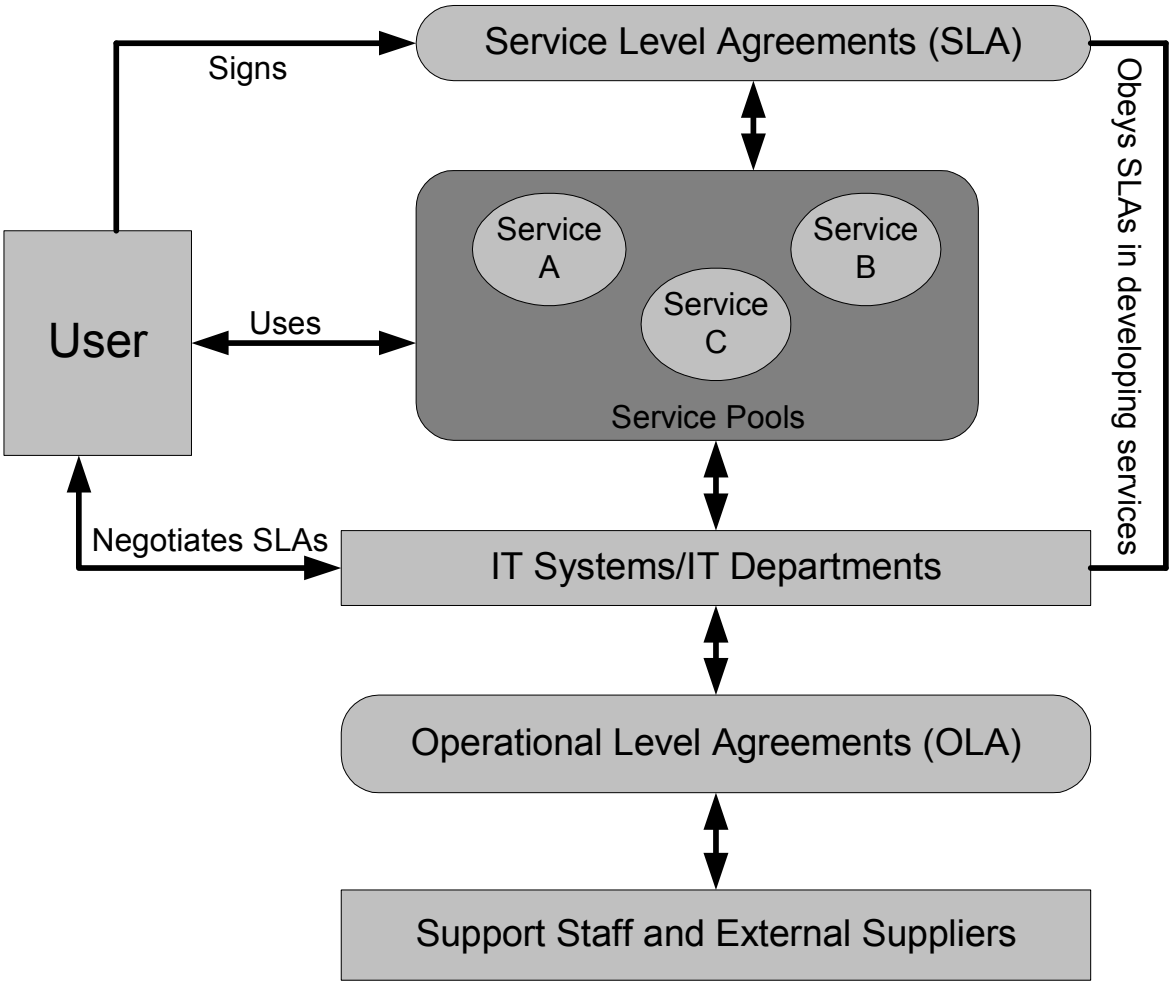

Figure 1.4.3, adapted from [12], shows agreement structures in Service Level Manegement (SLM)

b) **Availability Management** – ensures that services are always available wherever and whenever the customer needs them. This involves the reliability of the required services with customers happy to have no service at all other than a scrappy service, which frustrates the users. A typical example is the annoying NUL Internet service. So, availability management ensures that services meet the agreed standards documented in SLAs. The key elements of the availability management process are listed in [14] as follows:

- The percentage of agreed hours for which the service is available (Availability)
- Its reliability
- Its maintainability or the ability to restore services back to normal functioning
- Its serviceability or support capability from external suppliers
- Its security, consisting of confidentiality, integrity and access controls.

c) **Capacity Management** – this process covers the "*planning and managing to ensure the services meet the agreed levels in terms of performing at the required speeds and volumes*" [12]. In addition, capacity management ensures that future needs of the business, the customer and IT departments are forecasted and taken care of; i.e. scalability must be fitted into the services offered and into the SLA as well as OLA. Scalability is important because with time, businesses expand and more personnel are hired. "*The success of capacity management is very dependent on accurate forecasting of business needs, a good understanding of where technology is going and good planning for It capacity*" [14].

d) **Financial Management** – deals with provision of IT services within financial constraints of the company, i.e. the budget for IT must be respected when providing services. With financial management, the actual costs of providing IT services are identified and over-spending is avoided. There are three key processes involved in financial management as follows [12, 14]:

- Budgeting – "*the process of predicting and controlling how money is spent and consists of a periodic negotiation cycle to set budgets (usually annually) and the day-to-day monitoring of current budgets*" [12].
- Accounting – "*the set of processes that enable IT organizations to fully account for the way its money is spent*" [12].
- Charging – "*the set of processes required to bill customers for the services supplied to them*" [12].

e) **IT Service Continuity Management** – availability management ensures that services are always available, but does not cover major catastrophes such as fires, floods, earthquakes, terrorism, etc. These scenarios, with far-reaching consequences are covered by IT service continuity management. Several measures are taken to ensure services are brought back to normal as soon as

possible and such measures include: manual backups, intermediate recovery sites (warm standby) or even immediate recovery (hot standby) [14].

1.4.5. Service Support

Once quality, reliable services have been delivered, they have to be maintained and supported to preserve their agreed levels in SLA. So, service support is the key sub-module of service management, which "*describes the processes associated with the day-to-day support and maintenance activities associated with the provision of IT services*" [13]. As shown in figure 1.4.2, service delivery is composed of six processes as follows [12, 13, 14, 15]:

a) **Incident Management** – aims to protect service continuity by working quickly to restore normal service operation with minimal impacts to businesses and as soon as possible, after an incident that has caused service disruption. In [14], an incident is defined as "*any event that is not part of the standard operation of a service and which causes, or may cause, an interruption to or reduction in the quality of that service*".

b) **Problem Management** – deals with the actual causes of incidents. All errors that are known to have caused a problem are logged as "known errors" in the databases (CMDB) separate from the incidents that they cause. The log of known errors becomes helpful to non-skilled employees, who can solve incidents of known causes by just looking at the logs, and only those causes logged as unknown will need the expertise of IT professionals. So, problem and incident management are used for "*monitoring the infrastructure and resolving problems and disruptions to service*" [12].

c) **Configuration Management** – "*provides accurate information to support all the other service management functions*" [14], with the following objectives [12]:

- To identify and record the information required to manage IT services
- To identify control the information in the database (CMDB)
- To ensure that infrastructure information is up-to-date, and accurately reflects the actual infrastructure
- To provide a basis for the management of IT service management processes
- To provide information about the status of infrastructure components
- To provide a source for management information related to IT infrastructure management.

d) **Change Management** – is an ITIL process that deals with changes which might affect the delivery of a certain IT service, thus keeping the IT infrastructure in line with the needs of the business and advancement of technology. Any change requires the request for change (RFC) and follows a standardised procedure that goes through "Authorization" and "Approval". Change management has been summed in [12] as follows: "*to manage all changes that could impact on the IT department's ability t deliver services through standardized methods and processes, to*

ensure all change returns the correct value for expenditure, results in minimal disruption and is prioritized to produce optimal results for the organization".

e) **Release Management –** "*enforces effective use of any new or changed services that the organization plans to implement, and spans the planning, designing, building, testing and releasing of hardware and software components*" [14]. Together with change management, release management "*improves the infrastructure and services, providing the best return for effort and expenditure*" [12].
f) **Service Desk –** mostly referred to as help desk, provides the central contact point for customers to consult IT agents for everything concerning the IT services offered by the IT department. As opposed to other ITIL processes, identified in figure 1.4.2, service desk is a function [14], not a process, and "*provides an interface for all the other service support processes*" [13].

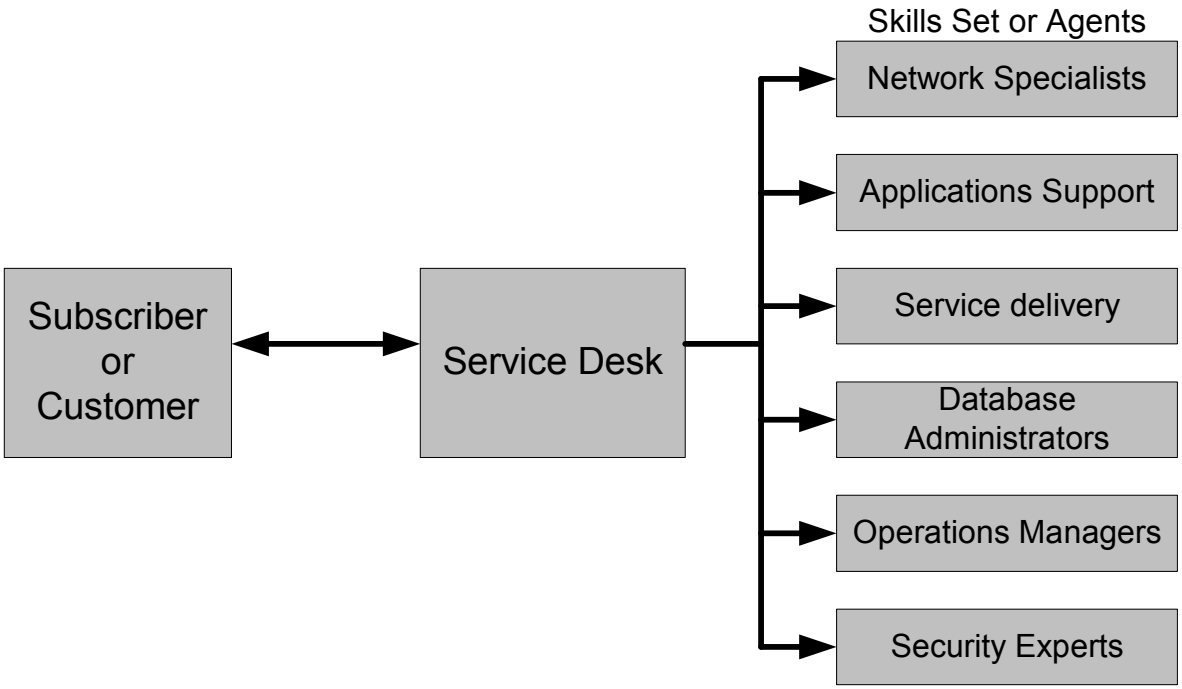

Figure 1.4.4, shows typical Service Desk deployments in most organizations

1.4.6. Service Desk

As already discussed, service desk is viewed as the primary contact for the customer but has several objectives including [12, 13]:

a) To drive and improve IT service on behalf of the business
b) To provide a point of contact where customers can report incidents and obtain assistance with the use of IT services
c) To accurately record information about IT incidents
d) To coordinate activity to restore normal service in terms of the SLA

e) To support the problem management process and provide an interface for all other service support processes
f) To provide management information about the performance and quality of IT services
g) To provide operational support to the business.

1.4.6.1. Benefits of a Service Desk

With service desk, incidents are reported and logged centrally thus providing the following benefits [12]:

a) Prevents the same incident being reported a number of times to different people
b) Prevents the loss of incidents
c) Prevents technical people being disrupted from important tasks
d) Prevents unnecessary work if the incident is already a known error.

1.4.6.2. Features of the Service Desk

No matter which structure the organization chooses, service desk should have the three key features namely [12]:

a) A single point of contact for all users – this point must aid communication with users, ensures that all incidents are recorded and allow better prioritization of technical staff's time.
b) A central log of all incidents with each incident being uniquely numbered and date/time stamped.
c) There should be diagnostic scripts, which include historical records and known error lists.

1.4.6.3. Service Desk Structures

There are three (3) types of service desks [12], namely: central, local and hybrid, and each is discussed next.

Central Service Desk

Calls are reported to a single service desk, with the first agent trying to resolve the problem, failing which the call is forwarded to the relevant skills set groups, as shown in figure 1.4.4. The first agent still monitors the call's progress until completion.

Advantages

Central service desk has the following advantages [12]:

a) Customers don't have to worry about who to call
b) Lower staff requirements – less personnel
c) More stable service levels through central control
d) Users need not known the field to which their problem falls

Disadvantages
Despite the benefits, there are also some downfalls of central service desk as follows [12]:

a) It is more difficult to maintain the training of staff in all the applications and support functions
b) Wider coverage can mean less depth of knowledge. This means that fewer incidents will be resolved at the first call
c) More need for specialists to assist the service desk agents.

Local Service Desk
Each skills set group has its own service desk, for example networking from figure 1.4.4, has its own service desk, so is applications support and all other groups as shown in figure 1.4.5.

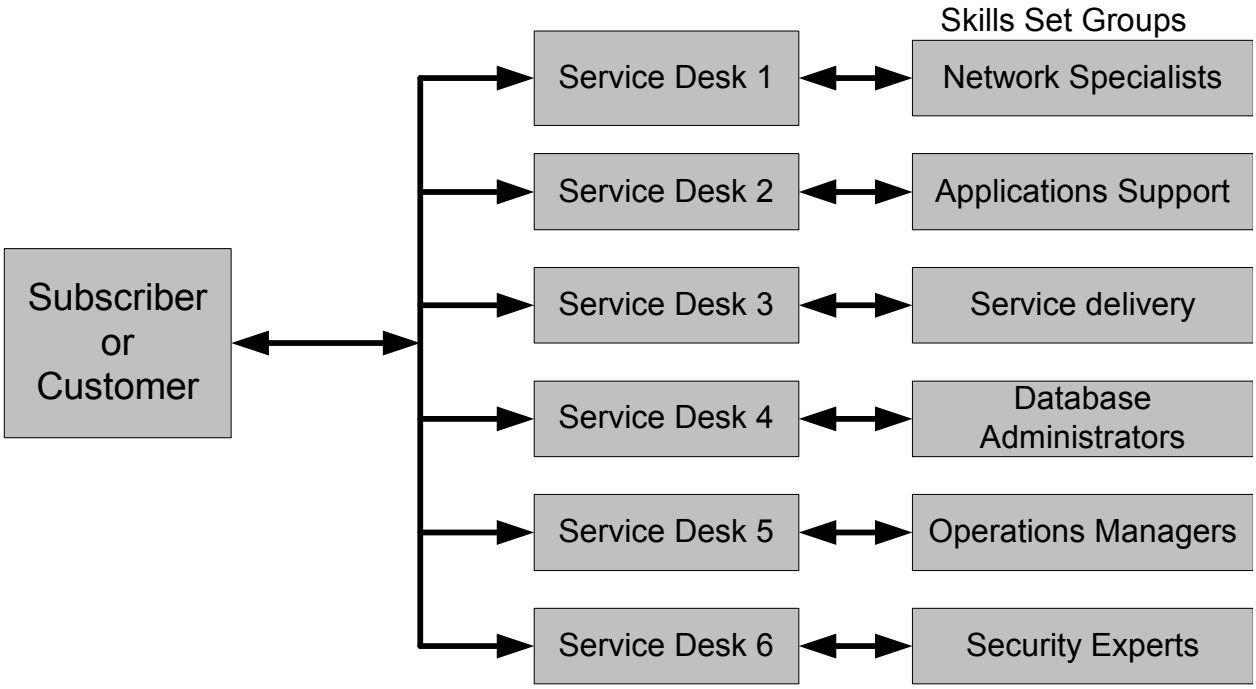

Figure 1.4.5, shows a local Service Desk Structure

Advantages:
Local service desk has the following advantages [12]:

a) Support can be customized to meet specific needs
b) Agents can develop a deeper knowledge bas due to the narrower focus of the service desk
c) Easier to maintain training for agents

Disadvantages:
Despite the benefits, there are also some downfalls of local service desk as follows [12]:

a) Customers must know which service desk to call, which could be confusing or even annoying to the user
b) Wrongful classification of the problem by the user can affect other service desks and their customers
c) Customers might queue for longer times only to discover, they waited for the wrong service desk.

Virtual Service desk
Virtual service desk is a hybrid structure of both central and local structure, while combining their benefits. From figure 1.4.6, a customer has to call only a single service desk, which is referred to as the primary service desk; if the agent cannot resolve the problem s/he passes it to the relevant secondary service desk, and if agents there are still unable to resolve the problem, then skill sets agents or specialists are involved.

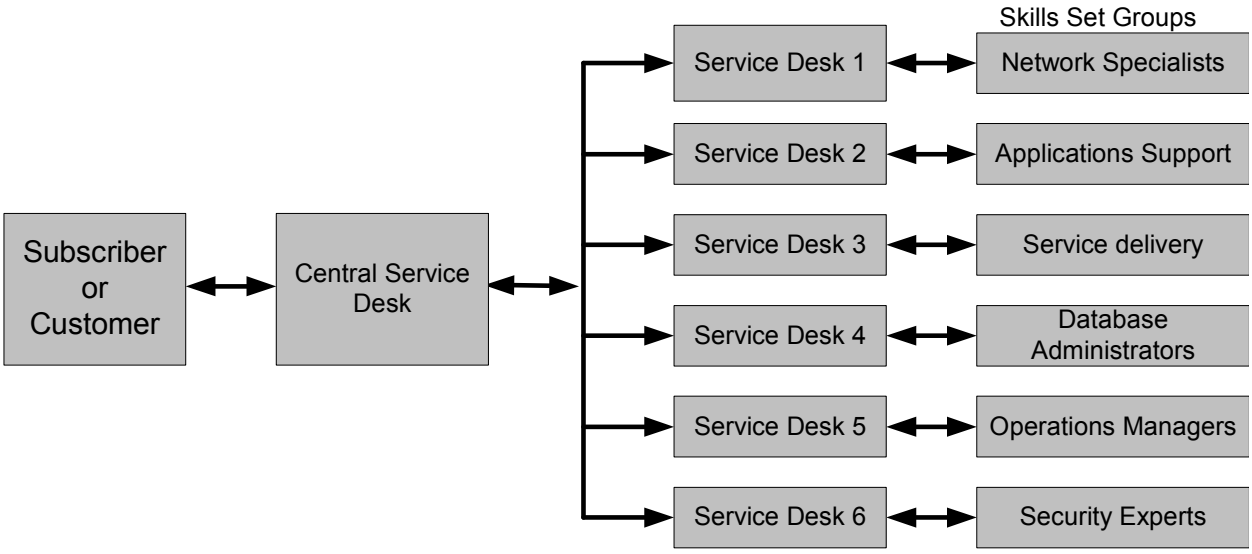

Figure 1.4.6, shows the Virtual Service Desk Structure

1.4.6.4. Types of Service Desks
Service desks are classified in [12] as follows:

a) *Technically unskilled* – a centralized service desk, which depends on known error lists to resolve problems, but does not give in-depth support and focuses more on coordinating and administrating incidents, problems and changes.
b) *Technical* – skilled agents in one or more areas are used and they aim to resolve most problems at first calls, however this may result in more users waiting in long queues.
c) *Expert* – aims to resolve all problem, thus requires experts which a huge skills base in different IT fields.

For further information on all the disciplines of service delivery and support under service management, consult [12].

Most businesses have a service desk equivalent in the form of "call centers". A call center answers calls, then routes calls to agents in a skillset that most closely meets the needs of the caller (customer or subscriber). If there are no agents available (i.e. all are engaged), the calls are placed in a queue to wait for an appropriate agent. Waiting callers receive periodic announcements and informative messages. Some "call centers" have automated responses for choosing the preferred language and for reporting the error or giving the user a predefined procedure if his or her problem has been resolved before. Call centers are used in telecomms companies, insurance companies, flight companies, etc. However, most call centers are not run properly and users are familiar with annoying responses like: "*Hello, your call is important to us, you are caller number 500,000, on the queue, please hold*"; then they play some music for the caller, though they don't even ask what kind of music one prefers, they assume their choice fits all. In some cases they are referred to as customer care centers and figure 1.4.7, shows a typical call center.

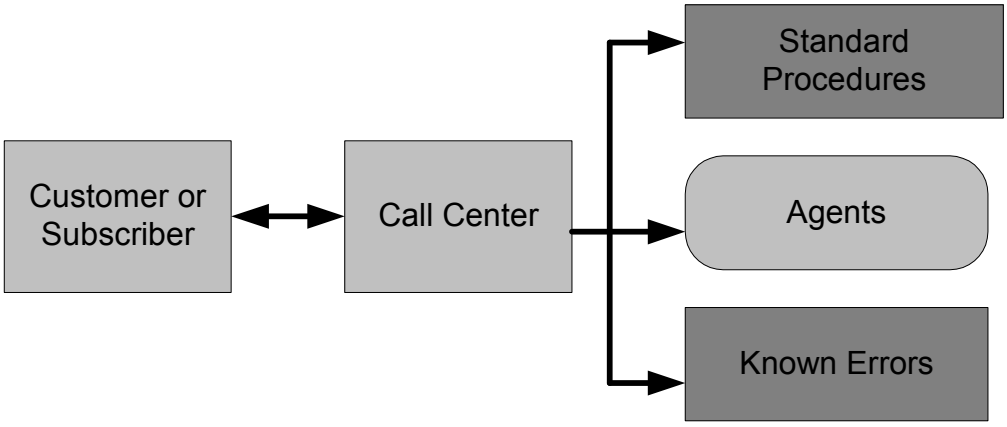

Figure 1.4.7, shows a Call Center Scenario

Example:
Vodacom Lesotho (VCL) call center or customer care center
Number: 114 from any Vodacom subscriber mobile set
Response: Welcome to Vodacom customer care, press:

- 1 for assistance in Sesotho
- 2 for assistance in English

After selecting a language, the following automated response takes place

- Press 0 – speak to a consultant
- Press 1 – port number
- Press 2 – SMS details and information
- Press 3 – prepaid account information
- Dial 133 – to retrieve voice messages

After pressing 0, if consultants are busy, you get a message telling you to wait for an available consultant.

1.4.7. Other ITIL areas

a) ICT Infrastructure Management (ICT IM) – from [13], ICT IM "*covers all aspects of ICT infrastructure management from identification of business requirements through the tendering process, to the testing installation, deployment, and ongoing operation and optimization of ICT components and IT services*"
b) Planning to implement service management – examines the issues and tasks involved in planning, implementing and improving service management processes within an organization. It also addresses the issues associated with addressing, cultural and organizational change, development of a vision and strategy and the most appropriate method of approach.
c) Application management – describes how to manage applications from the initial business need, through all stages in the application lifecycle, up to and including retirement; with great emphasis on ensuring that IT projects and strategies are tightly aligned with those of the business, throughout the application lifecycles, to ensure that the business obtains best value from its investment.
d) The business perspective – provides advice and guidance to help IT personnel to understand how they can contribute to the business objectives and how their roles and services can be better aligned and exploited to maximize that contribution.
e) Security management – details the process of planning and managing a defined level of security for information and IT services, including all aspects associated with reaction to security incidents. It also includes the assessment and management of risks and vulnerabilities and the implementation of cost justifiable countermeasures.

Full chapters on all these ITIL books can be found in [13].

Assignment 1 (2007 First Semester):

Identify and discuss services offered by the CSU at NUL. In your discussion look into the relevance of those service to NUL objectives and goals; identify infrastructure needed to support each service; their reliability, availability and quality of service. In addition to the services, study the CSU Service desk and classify it based on the types identified under section 1.4, and investigate how calls are handled by the service desk.

1.5. Standards in Telecommunications

> *"Telecommunications is essentially a global business. Significant amounts of traffic crosses national boundaries and substantial amounts of technology are exported from a source country to a user country. Standardization of all functional aspects of telecommunication systems is therefore essential" [19]*

1.5.1. Introduction

Telecommunications and networking involve transmission of information from point A to point B, over several media ranging from wireless to wired. The equipment involved is from different vendors and manufacturers. Also systems developed to work over the network are developed by different service developers, but they have to be accessible to everyone on the network form local market to international market. So, when developing new products for the international market, service providers have to bear in mind compatibility issues. In addition, there is always a need for one's products to interconnect or interwork with other products on the market. To ensure that there is compatibility and interworking among electronic components, all product developers must adhere to certain international agreed upon specifications, so that every user on the international market can freely buy any product and enjoy its full capabilities without any restrictions. Typical problems with similar products from different competing companies include the electrical wall sockets; some are rectangular, while others are round, and each needs its own plug.

To avoid these problems, network elements and interfaces in telecommunications are standardized to open competition among suppliers, so that customers get used to choice based on their needs. With telecommunications standardization, typical questions such as "*is transmitting hardware purchased from one vendor work correctly with receiving hardware purchased from another vendor?*" [5] are avoided, as all vendors have to adhere to certain agreed specifications. There are several reasons for standards including:

a) Equipment interoperability
b) Systems and service compatibility
c) Interworking of systems, equipment and services
d) Avoiding vendor lock-in
e) Increased international market competition
f) Limits use of proprietary systems
g) Fast technology development and adoption as all vendors work with the same specifications.

The main aim of standards is to "*ensure that communication hardware built by different vendors will interoperate*" [5]. So, standards are the documents which contain specifications about a certain technology. In the previous sections, several documents known as "*recommendations*" have been referenced; so, a "*recommendation*" is "*a piece of advice, usually contained in documents as well, which if followed by the majority will be adopted*

as a standard" [4]. So, some recommendations make it as standards while others remain recommendations, which are weaker than standards. Though adhering to standards and recommendations is voluntary, authorities have ways of forcing suppliers to adhere to them including the following demands [4]:

a) If the standard/recommendation is not adhered to, your product cannot be offered for sale on our markets;
b) If your telephone system does not comply with the standard/recommendation, you will not be allowed to connect it to the international network;
c) If you do not refer to this specific standard/recommendation, we cannot take your tender into consideration;
d) Etc.

If however a company creates a completely new product and that product rapidly penetrates the market, that product gains what is called a "*de facto*" standard [4]. So, according to [4], a company can create de facto standard:

a) If there are no standards
b) If the product is the first of its type on the market
c) If the product is a key product
d) If the product captures a sufficiently large share of the world market.

1.5.2. Stakeholders in Standards

Stakeholders in this context refer to all parties involved in standards (*i.e. have an interest in standards activities*) and affected by the implementation of standards, whether by benefiting or being disadvantaged. There are three [4] key stakeholders which are:

a) Authorities – standards are of importance to different authorities who actually participate in their creation due to the following societal and commercial objectives [4]:

    i. To protect the safety of the citizens
    ii. To avoid technical barriers to trade in the form of different national requirements
    iii. To encourage the development of technologies and markets
    iv. To ensure fair competition and adoption of new technologies for the benefit of customers.

b) Users – standards help users to avoid vendor lock-in and enables them to enjoy the following [4]:

    i. It must be possible to use different makes together
    ii. Products must be capable of being used world wide
    iii. Competition between two or more suppliers makes a product less expensive

iv. Cooperation during the standardization phase favors the choice of a good solution.

c) Suppliers – authorities and users actually benefit from standards whereas suppliers are affected by standards in a negative way as they rather sell a de facto standard; however their participation ensures [4]:

i. Competition on equal terms
ii. Larger manufacturing volumes
iii. New or large markets
iv. More efficient research and development

1.5.3. Organizations involved in Standards

Several organizations are involved in standardization and can be grouped into international or regional. International organizations are mainly concerned with standards that affect the entire international market, i.e. globally; while regional organizations develop standards based on the need of their regions, however they still have to observe the international standards in order to avoid any conflicts between the two. Regional organizations are grouped according to continents, however, a standard developed for Europe can be adopted for Africa as is currently the practice, that means though developed for certain regions they still can be applied to other regions.

International Telecommunications Union (ITU)

ITU [4, 5, 17, 18, 19] established in 1865 [4, 17, 18], with headquarters in Geneva Switzerland [4, 17], is "*an agency of the United Nations that coordinates the establishment and operation of global telecommunication networks and services*" [18]. It is formed by governments, private sector organizations, telecommunication companies and individuals from all UN member nations and is funded through voluntary member fees. ITU has several activities including [18]: "*the coordination, development, regulation, and standardization of international telecommunications as well as the coordination of national policies. In addition, it provides technical assistance to developing countries in the area of telecommunications*" [4]. And its goals are "*to foster and facilitate the global development of telecommunications for the universal benefit of mankind, through the rule of law, mutual consent and cooperative action*" [18]. In 1993 [4], the ITU was divided into three sectors, and each of these sectors has several study groups.

Telecommunications Standardization Sector (ITU-T) – formerly the Consultative Committee for International Telephony and Telegraphy (CCITT) [4, 5, 18, 19], is responsible for international coordination of all telecommunications traffic and produces standards for this purpose. ITU-T has fifteen study groups including [4, 17]: service definition, network operation, television and sound transmission, tariff and accounting principles, etc. Examples of standards from ITU-T include X.25, G.803 – SDH transport network architecture, etc.

Radiocommunication Sector (ITU-R) – responsible for coordinating the use of radio frequencies [4, 18, 19]; and "*satellite orbits, finite natural resources which are increasingly in demand from a large number of services such as fixed, mobile, broadcasting, amateur, space research, meteorology, global positioning systems, environmental monitoring and, last but not least, those communication services that ensure safety of life on land, at sea and in the skies*" [17].

Development Sector (ITU-D) – undertakes commitment of the ITU to development projects in the area of telecommunications and to manage UN-financed development projects in developing countries; example projects include: "*Digital Divide – Connecting the Unconnected by 2015*" [17].

[***ITU URL***]: http://www.itu.int; Last Accessed 25th July 2007

International Organization for standardization (ISO)

ISO [4, 5, 18, 19], established in 1947 [18] is a "*worldwide federation of national standards bodies with representatives from over 100 countries*". It's a non-governmental organization with a mission: "*to promote the international exchange of goods and services and to develop cooperation in the spheres of intellectual, scientific, technological and economic activity*" [18]. Example standards from ISO include OSI reference model, a seven layer model which, promotes open networking environments that let systems from different vendors to communicate using internationally accepted protocols.

[***ISO URL***]: http://www.iso.org; Last Accessed 25th July 2007.

Internet Engineering Task Force (IETF)

IETF [5, 18], is "*a large open international community of network designers, operators, vendors and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet*" [18]. More on IETF can be found at: http://www.ietf.org.

Joint Technical Committee 1 (JTC1)

JTC1 [4], is an international organization formed in 1987, as a joint venture between ISO and International Electrotechnical Commission (IEC), in the area of information technology (IT).

Asynchronous Transfer Mode (ATM) Forum

Due to delays and slow operation of ITU and JTC1, special standardization bodies have been formulated to speed up the process and cover new fields, which have no representatives in both bodies. ATM forum is an example of such special bodies and in cooperation with ITU-T develops ATM standards [4].

European Telecommunications Standards Institute

ETSI [4, 19] replaced CEPT in 1988 [4] as the official European organization for telecommunications standardization, and has a task of creating standards for the European common market, but which are also internationally adoptable. Due to

monopolistic markets, its predecessor CEPT only had telecommunications administrations as its members, however ETSI membership include [4]: administrations, network operators, service providers, manufacturers and users, each with direct influence on standardization work. To perform its work effectively, ETSI has several technical committees composed of highly qualified experts and consultants.

Institute of Electrical and Electronics Engineers

IEEE [4, 18], is a society based in North America and develops several standards for data communications. Their standards are first developed as LAN drafts, which are then passed on to ANSI for approval and standardization in the US and also forwards drafts to the ISO. Several standards from IEE include: IEEE 802.3 – Ethernet; IEEE 802.16 – WiMax; IEEE 802.11 – WLAN; IEEE 802.20 - WMB; IEEE 802.15 – Bluetooth; IEEE P1675 – Broadband over power line hardware; IEEE P1901 – MAC and physical layer specifications for all access BPL devices; IEEE BPL – Standardization of broadband over power line technologies; IEEE P1775 – PLC equipment, electromagnetic compatibility requirement, testing and measurement methods.

Telecommunications Industry Association

TIA [4, 18], based in the US, acts as a voice for the communications and IT industry, with membership ranging from vendors, service providers, up to organizations that are involved in all aspects of modern communication networks. TIA works in partnership with Electronic Industries Association (EIA) [5, 18], to develop networking standards for cabling buildings in the US, and one example is the TIA/EIA 586 A or B – straight through networking cable, already encountered in 3rd networking course.

American National Standards Institute

ANSI [19, 19], a USA organization which founded ISO and is one of the five permanent members of ISO. It also represents the USA in both ITU and ISO, and "*promotes the use of US standards internationally, advocates US policy and technical positions in international and regional standards organizations, and encourages the adoption of international standards as national standards where these meet the needs of the user community*" [18].

Other regional bodies include committee for telecommunications (CT1) in USA; Telecommunications Technology Council (TTC) in Japan; Research and Development Center for Radio Systems (RCR) in Japan; etc.

1.6. Telecommunications and Regulation

1.6.1. Introduction

Several definitions of the word "*regulation*" can be found on the web, but for CS5440 course, the following definition is adopted: "*rules enforced by a government agency to restrict or control economic activity in price setting, product standards, and the conditions under which firms/companies can enter an industry*". From thus definition it's clear that any new player in a certain field has to satisfy certain requirements before it can be allowed by a governing body to participate in that market sector, whether local or international. Just like all sectors of industry, telecommunications is regulated, though previously, the regulations were there to mainly restrict new players entering the market as there were monopolies; such as Telecom Lesotho in Lesotho until 2007, AT&T in USA until 1984 [20], Telkom SA in South Africa until 2006 when the SNO in the name of Neotel was introduced. In monopolistic cases, governing bodies only have to be concerned about tariffs, meeting agreed targets and barring all new players, hence no competition to worry about. Most of these monopolistic companies are state owned, examples include Telecom Lesotho which was government owned before being privatized but still government has shares, the same goes for Telkom SA, where SA government has *38%* shares. With monopoly, only one service provider serves all the users in a particular country. Regulations during monopoly times were mainly about restrictions in the telecommunications sector, e.g. for a certain period of time only this operator is allowed exclusive rights, VOIP is illegal during this period, etc.

Several reasons have been put in [20] for having telecommunications regulations including:

a) Desirable competitive outcome could not be achieved by market forces
b) The regulator can help the industry achieve technical compatibility and avoid fragmentation
c) Society needs to be protected from the industry in terms of affordable prices and high quality of service.

The roles of governments in telecommunications regulations and industry as a whole has mixed results, mainly because governments are about politics, so this political intervention is a really unwanted incentive in the growth of the industry. Though in some cases such as the need for "*emergency services*", which most governments deem as essential to all, are beneficial to both society and the industry.

In most countries, the legal and economic frameworks within which telecommunications industries operate has undergone significant changes with the trends being from the privatization of state telecommunications companies; to breakdowns of the monopolies; to deregulated environment that encourages competition [19]. Deregulation does not necessarily refer to the removal of laws, but

simply defines the relaxation of entry criteria used in the telecommunications industry and it's formally defined for CS5440 as: "*the progressive removal of controls on entry and operations, intended to enhance competition and raise the productivity of the major entities in the telecommunications industry*". In a deregulated environment, multiple service providers offer their services competitively to their customers. So, currently the world is moving towards a deregulated, competitive market as opposed to the previous regulated, monopolistic market, and all this means is happier customer, with access to the latest technology, not technology that a provider wants to provide. Differences between the two markets are summarized as table 1.6.1.

Monopolistic	Competitive
No Competition (Monopoly)	Highly Competitive
100% Market Share (one Operator)	Dynamic Market Share (More operators)
Services are based on technological capabilities	Services are based on customer needs (Customer is King scenario)
No competitive pull for new services	New services are key to market share
Regulated Market	Deregulated Market

Table 1.6.1, adapted from [19], shows the changing telecommunications market

From table 1.6.1, it's clear that historically the customer had no say as to which services they wanted to subscribe to and were left to pay for the services offered by the monopoly at the price that suited the monopoly, and left them (subscribers) disadvantaged. This in turn resulted in slow penetration of telecommunications and ICT as a whole. Realizing that telecommunications was very significant in economic development, most countries are now adopting the deregulated, competitive market in an effort to increase ICT penetration and to reduce the digital divide and also help speed up projects like "*Digital Divide – Connecting the Unconnected by 2015*" [17]. In addition, a deregulated market leads to reduced prices for services, which in turn leads to more access to ICT and improved social and economic human lifes.

Exercise:
Identify at least three (3) economic and three (3) social benefits of telecommunications.

1.6.2. *I*ndependent *C*ommunications *A*uthority of *S*outh *A*frica

ICASA [21] established by ICASA Act No.13 of 2000 [21] to replace the ***S***outh ***A***frican ***T***elecommunications ***R***egulatory ***A***uthority (SATRA), is the regulator for the South African communications sector responsible for the regulation of broadcasting and telecommunications services. It licenses telecommunications and broadcasting service providers, monitors compliance of licensees against license conditions, develops policy, manages the frequency spectrum and protects consumers within the communications

environment [21]. Though proclaimed to be independent, the SA government through the minister of communications, DR. Ivy Matsepe-Casaburri, makes amendments to the telecommunications act, examples being: leasing of spare capacity from Municipalities to VANs and other licensed operators; legalizing of VoIP in SA.

ICASA has a mission "*to regulate the communications industry for the benefit of stimulating economic growth and contributing to the country's social development*" [21]; to achieve this mission, ICASA set the following goals [21]:

a) Create a competitive environment for the communications industry,
b) Attractive domestic and foreign investment for the industry,
c) Foster innovation and choice for consumers,
d) Promote choice and diversity of content,
e) Promote universal service and access.

More information on ICASA can be found in [21]

1.6.3. *L*esotho *T*elecommunications *A*uthority

LTA [22] is a statutory body responsible for the regulation of the telecommunication sector in Lesotho, established by the Lesotho Telecommunications Act of 2000(Amended 2001). LTA has a vision [22] "*be an efficient and financially sustainable telecommunications regulator recognized for excellence nationally, regionally and internationally for a regulatory framework that meets consumer, investor and Government expectations*"; and has the following objectives [22]:

1. To promote universal access to Info-Communications Technology (ICT) services and universal service to basic telecommunications service.
2. To enforce and foster free and fair competition within telecom markets in promoting efficient prices, efficient supply of service, good quality of service, and advanced ICT services. Where competitive markets do not exist or fail, to prevent abuses of market power such as excessive pricing and anti-competitive behavior by dominant firms.
3. To create a favorable climate that will promote investment within the telecommunications sector.
4. To promote public confidence in telecommunications markets through transparent and predictable regulatory and licensing processes as well as protecting consumer rights.
5. To promote opportunities for all Basotho to benefit from the information revolution with particular attention to women and the disabled
6. To optimally manage the use of scarce resources such as the radio spectrum, numbers and rights of way.
7. To ensure efficient interconnection arrangements that promote increased telecommunications connectivity for all users.

8. To ensure relevant and appropriate broadcasting services are extended to all citizens.

LTA regulates two sectors namely [22]:

a) **Telecommunications** – with several companies including: Telecom Lesotho (fixed line); Vodacom Lesotho (mobile); Econet Ezi-Cel Lesotho (mobile); and Bethlehem Technologies (Internet and Broadcasting Carrier).
b) **Broadcasting** – Television: TV Lesotho and TBN Lesotho; and Sound broadcasting: Radio Lesotho, CRFM, Joy, PC FM, Mo-Afrika, Harvest, etc.

More information on LTA can be found in [22]

1.6.4. *Of*fice of *Com*munications (Ofcom)

Ofcom [23], established by the office of communications Act 2002, is the UK regulator in communications industries with responsibilities across: television, radio, telecommunications and wireless communications services. Ofcom practices the freedom of information act of 2000, thus allowing anyone to ask for information in its possession. Ofcom duties have been split into six areas as follows [23]:

1. Ensuring the optimal use of the electro-magnetic spectrum
2. Ensuring that a wide range of electronic communications services - including high speed data services - is available throughout the UK
3. Ensuring a wide range of TV and radio services of high quality and wide appeal
4. Maintaining plurality in the provision of broadcasting
5. Applying adequate protection for audiences against offensive or harmful material
6. Applying adequate protection for audiences against unfairness or the infringement of privacy

Unlike most telecommunications regulators in other countries, including Lesotho and SA, Ofcom was formed by the involved players in telecommunications in the UK, not members chosen by governments or other criterion. This ensures that the regulator truly has the telecommunications industry's interests at heart and fully understands major technologies before ruling over them or setting policies to guide them. In addition Ofcom first researches and tests most technology advances before the actual players can be involved and their policies are then based on informed and not political decisions. Most countries are advised to follow Ofcom's example if they want to speed up ICT penetration and to fairly judge over conflicts in the deregulated market.

More information about Ofcom can be found in [23].

1.7. Network Model and User Services

1.7.1. Network Model

The network model adopted in CS5440 is shown in figure 1.7.1. The model does not discriminate the network (either voice or data), that is both data networks and voice networks follow the same model.

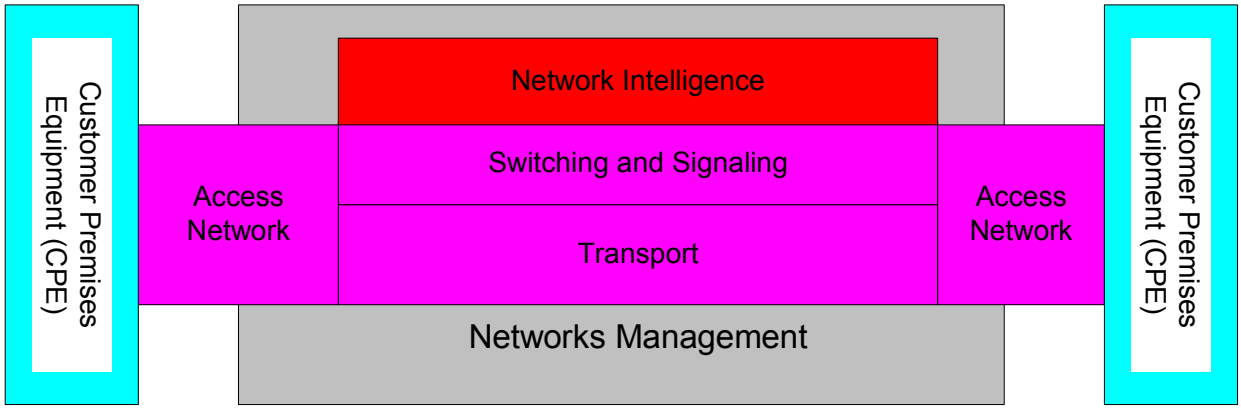

Figure 1.7.1, adapted from [4], shows the network model used in Networks Management (CS5440) course at NUL

From figure 1.7.1, first layer (group of devices), which the user interacts with directly is the customer premises equipment (CPE) and include devices such as TV sets, PCs, telephone sets, mobile phones, PDAs, laptops, etc; plus access units such as modems and adaptors. The first set of customer premises equipment is often referred to as end-user terminals. From there, the access network layer links the customer premises equipment with the service provider's network and several technologies used include: 2G, 2.5G, 3G, 4G, cable modem, cable TV, xDSL, ISDN, PLC, Wi-Fi, satellite, WLL, fiber technologies, etc. The transport network layer, referred to as the transmission network transports traffic from access networks to the core network (backbone/backhaul) network, which then takes the aggregated traffic and transports it to networks from other service providers. In figure 1.7.1, transmission and core networks are combined under the transport layer, and example technologies include: IP MPLS, ATM, fiber, WiMAX, satellite, SDH, PDH, etc.

The switching and signalling layer is involved with finding appropriate routes to subscribers and directing traffic to the appropriate exchange. Before directing traffic to the correct exchange, data about the location is maintained through signalling and two technologies to be discussed in this course are SS7 and SIP. Network intelligence layer deals with all those supplementary or additional services offered by other networks, which rely on the databases to store advanced routing and switching functions. Examples of services include: freephone, local number portability, premium rating, telephone call screening, three way party calls, call waiting, call divert, etc. networks management layer covers all other layers and deals with monitoring, supervision and

control of other layers. The management standards discussed already include TMN, ISO, ITIL, SNMP, RMON, etc. All other network equipment in all the layers needs to be monitored for efficient operation.

1.7.2. User Services

The key purpose of any telecommunications network is to provide services to network users, "subscribers" or "customers". Services can be classified as [4, 19]:

a) **Bearer service –** a type of telecommunications service that provides the capability for the transmission of signals between user-network interfaces; i.e. it only provides the "*transport system*" for exchanging information. Example is the telephone network, which is the carrier of the actual service called telephony. These networks are called "bearer networks" and have the following plans [4]: numbering, charging and transmission.
b) **Teleservice –** a type of telecommunications service that provides the complete capability, including terminal equipment functions, for communications between users according to protocols established by agreement. In short, a Teleservice is just "a bearer service plus terminal capability". Examples include: telephony, SMS, MMS, fax, emergency calls, etc.

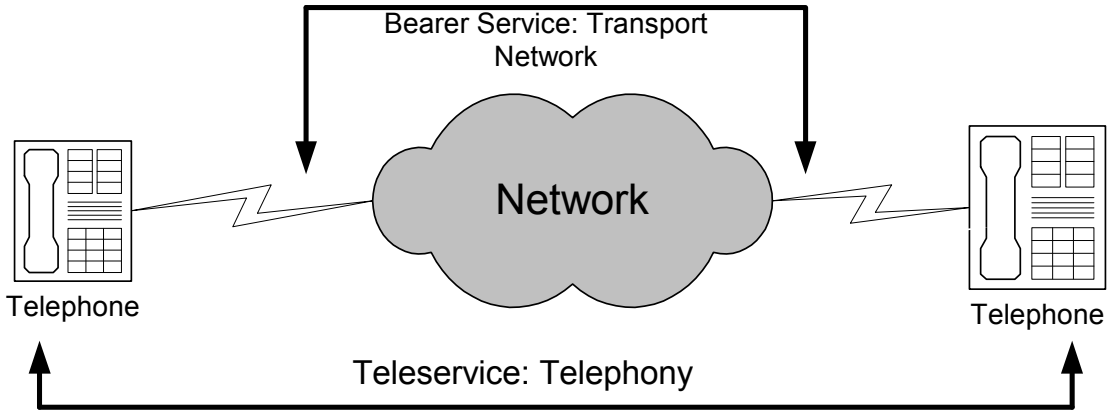

Figure 1.7.2, [4], shows differences between bearer and teleservices

c) **Value- added services –** services involving processing information, which enhances the value of the service beyond that of the basic telecommunications bearer function.

From the operator's point of view a Teleservice is divided into the "basic service" and "supplementary services". All users of a teleservice have access to the basic service, which in telephone systems is the actual telephony. The provision of "extra services" beyond the basic service constitutes value-added services. Value-added services are offered either by the operator or the third party service provider, for a special fee.

Examples include: directory enquiry services, stock exchange information, weather, forecasts, etc. Supplementary services – modification of the basic service, i.e. enhanced network capability. Examples include: caller identification; call forwarding; call waiting; alarm call/reminder; credit card calls, etc. In addition to the already discussed classifications, services are classified based on their time requirements as follows [19]:

a) *Real-time services* – also called synchronous services, require the information to be transmitted and delivered within stated time limits; e.g. telephony.
b) *Non-real time services* – also called asynchronous or deferred services, do not have stated time limits for delivery of information; e.g. web browsing, SMS.

From the user's point of view, teleservices are classified based on the form in which information is presented, as follows [4]:

a) Voice
b) Data – including text
c) Video – moving pictures and sound
d) Multimedia – "*a service which contains at least two of the three service types – voice, data and video, and which provides a certain degree of interactivity*".

These four service types are further subdivided based on the way services are handled with respect to the user as follows [4]:

a) *Interactive services* – two-way transmission of information.
   - Voice – telephony
   - Data – computers communicating over a network; withdrawing money from the bank ATM
   - Video – videoconferencing
   - Multimedia – videoconferencing
b) *Messaging services* – storing information for later references
   - Voice – voicemail
   - Data – telex, SMS, E-mail, electronic data exchange
   - Video – video mailbox (future application)
   - Multimedia – Due to the need for interactivity, there are no messaging services for multimedia.
c) *Retrieval services* – services that provide access to information stored in databases
   - Voice – weather forecasts, sports results, etc
   - Data – www/internet services
   - Video – internet services which include video
   - Multimedia – video-on-demand and TV recordings provided by PVR decoders
d) *Distributive services* – two types: one-way communication to a single receiver (telefax) and one-way simultaneous communication to multiple receivers (Radio and TV).

- Voice – broadcasting: Radio and TV
- Data – telefax, news on TV (News24 on DSTV channel 59); teletext
- Video – TV broadcasting
- Multimedia – video-on-demand.

1.8. References

[1]. M.3010, "*Principles for a telecommunications management network*"; February 2000, ITU-T Recommendation M.3010.

[2]. M.3400, "*TMN management functions*"; February 2000, ITU-T Recommendation M.3400.

[3]. M.3016, "*TMN security overview*"; June 1998, ITU-T Recommendation M.3016.

[4]. A.Hellman and G.Bager, "*Understanding Telecommunications 1*", Ericsson Telecom, Telia and Studentlitteratur, 1997; ISNB: 91-44-00212-2.

[5]. D.E. Comer, "*Computer Networks and Internets*", Second Edition; Prentice Hall, Inc, 1999; ISBN: 0-13-083617-6.

[6]. A. Pras, "*Network Management Architectures*", Centre for Telematics and Information Technology; Netherlands, 1995; ISBN: 90-365-0728-6.

[7]. IEC, "*Element Management Systems*", Web ProForum Tutorials; http://www.ies.org; Last Accessed 12 June 2007.

[8]. B. Ratner and A. Huckridge, "*Testability in the NGN*", MSF Technical Report; MSF-TR-ARCH-006-final; Septermber 2005.

[9]. B. Waker, "*The Art of Production Environment Engineering*"; Sun Microsystems, Inc; 1 June 2000.

[10]. D. Kakadia; "*Enterprise Management Systems Part 1: Architectures and Stsndards*"; Sun Microsystems, Inc; April 2002.

[11]. Flexitronics, "*FCAPS*", Flexitronics Software Systems Whitepaper, 2005.

[12]. CSMG, "*IT Service Management*"; ITIL Foundation Course; CSMG 2000 – 2004.

[13]. C. Rudd, "*An Introductory Overview of ITIL*"; Version 1.0a, ItSMFLtd, 2004.

[14]. J. Murray, ""*An Introduction to ITIL Concepts*", October 2005; http://devresource.hp.com/drc/resources/itilconcepts/ITILconcepts.pdf; Last Accessed 14 June 2007.

[15]. "*ITIL Essential Study Guide*"; http://www.unl.edu/remedy/presentations/itil_guides.pdf; Last Accessed 14 June 2007.

[16]. J. Parker, "*FCAPS, TMN and ITIL – three key ingredients to effective IT management*"; 6 May 2005, OpenWaterSolutions, LLC.

[17]. International Telecommunications Union (ITU) homepage; http://www.itu.int; Last Accessed 14 June 2007.

[18]. T. Sheldon, "*Encyclopedia of Networking*", Electronic Edition; Osborne McGraw-Hill, 1998; ISBN: 0-07-882333-1.

[19]. H.E. Hanrahan, "*Integrated Digital Communications*"; School of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg, 2006.

[20]. N. Economides, "*Telecommunications Regulation: An Introduction*"; Stern School of Business, New York University; June 2004.

[21]. ICASA Website; http://www.icasa.org.za; Last Accessed 27 July 2007.

[22]. LTA Website; http://www.lta.org.ls; Last Accessed 27 July 2007.

[23]. Ofcom Website; http://www.ofcom.org.uk; Last Accessed 29 July 2007.

[24]. S. Aidarous and T. Plevyak, "*Principles of Network Management*"; Chaper 1.

[25]. X.700, "*Management Framework for Open Systems Interconnection (OSI) for CCITT Applications*"; ITU Recommendation X.700, September 1992.
[26]. David Carte; "*Trading on JSE Resumes, Will Continue until 19h00*"; July 14, 2008; http://www.moneyweb.co.za/mw/view/mw/en/page38?oid=214866&sn=Detail; Last Accessed August 18, 2008.
[27]. Airline Industry Information; "*Delays reported at Heathrow Airport due to computer crash*"; M2 COMMUNICATIONS LTD; February 21, 2008; http://findarticles.com/p/articles/mi_m0CWU/is_2008_Feb_21/ai_n24318922; Last Accessed August 18, 2008.
[28]. DHD Multimedia Gallery; "*Bizarre Airport Computer*"; http://gallery.hd.org/_c/bizarre/airport-computer-crash-Where-did-you-want-to-go-today-ANON.jpg.html; Last Accessed August 19, 2008.
[29]. Reuters; "*JSE Shakes Off Technical Glitch*"; News24; July 12, 2010.